FISH & RICHARDSON P.C.

225 Franklin Street
Boston, Massachusetts
02110-2804

Telephone
617 542-5070

Facsimile
617 542-8906

Web Site
www.fr.com

Frederick P. Fish
1855-1930

W.K. Richardson
1859-1951

April 2, 1999

Attorney Docket No.: **10360/023001**

Box Patent Application
Assistant Commissioner for Patents
Washington, DC 20231

Presented for filing is a new original patent application of:

Applicant: MATTHEW W. POISSON, MELISSA L. DESROCHES, JAMES M. MILILLO, RAVI SUBBARAO

Title: MONITORING A VIRTUAL PRIVATE NETWORK

BOSTON
NEW YORK
SILICON VALLEY
SOUTHERN CALIFORNIA
TWIN CITIES
WASHINGTON, DC

Enclosed are the following papers, including those required to receive a filing date under 37 CFR §1.53(b):

	Pages
Specification	22
Claims	4
Abstract	1
Signed Declaration	[To Be Filed At A Later Date]
Drawing(s)	40

Enclosures:

- Postcard.
- Appendix A (8 pages); Appendix B (16 pages); Appendix C (13 pages).

Basic filing fee	760.00
Total claims in excess of 20 times $18.00	0.00
Independent claims in excess of 3 times $78.00	156.00
Fee for multiple dependent claims	0.00
Total filing fee:	$ 916.00

Under 37 CFR §1.53(d), no filing fee is being paid at this time. Please apply any other required fees, **EXCEPT FOR THE FILING FEE**, to deposit account 06-1050, referencing the attorney docket number shown above. A duplicate copy of this transmittal letter is attached.

"EXPRESS MAIL" Mailing Label Number EL182578396US

Date of Deposit April 2, 1999

I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as **"Express Mail Post Office To Addressee"** with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Alison Brazil

Alison Brazil

If this application is found to be incomplete, or if a telephone conference would otherwise be helpful, please call the undersigned at 617/542-5070.

Kindly acknowledge receipt of this application by returning the enclosed postcard.

Please send all correspondence to:

Denis G. Maloney
Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804

Respectfully submitted,

Robert A. Greenberg
Reg. No. 44,133
Enclosures

365890.B11

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: **MONITORING A VIRTUAL PRIVATE NETWORK**

APPLICANT: **MATTHEW W. POISSON**
MELISSA L. DESROCHES
JAMES M. MILILLO
RAVI SUBBARAO

"EXPRESS MAIL" Mailing Label Number EL182578396US

Date of Deposit April 2, 1999

I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as **"Express Mail Post Office To Addressee"** with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Alison Brazil

Alison Brazil

Monitoring a Virtual Private Network

Background

This invention relates particularly to monitoring a virtual private network.

LANs (Local Area Networks), Intranets, and other private networks interconnect user computers, file servers, e-mail servers, databases, and other resources. Typically, organizations want to offer remote access to private network resources to traveling employees, employees working at home, and branch offices without compromising the security of the private network.

Virtual private networks (a.k.a. Extranets) securely stitch together remote private networks and remote computers using a public network such as the Internet as a communication medium. Each private network can connect to the public network via an extranet switch such as the Contivity™ Extranet switch offered by Nortel™ Networks. Extranet switches provide a variety of virtual private network functions such as network packet tunneling and authentication.

For configuring the functions provided by the switch, Contivity™ switches offer a web-server and web-pages programmed to configure the different virtual private network functions in response to administrator interaction with the web-pages. By using a browser to navigate to each virtual private network switch, one after another, the administrator can configure the tunneling, authentication, packet filtering, and other functions provided by the switch. Management functions provided by the Contivity™ switches are described in greater detail in the New Oak™ Communications Extranet Access Switch Administrator's Guide.

Summary of the Invention

In general, in one aspect, the invention features a method of managing a virtual private network that includes receiving information describing at least one virtual private network attribute from multiple computers providing at least one virtual private network function, preparing a report by organizing the received information into a table that lists each of the multiple computers and the corresponding virtual private network attribute received from each of the multiple computers, and displaying the prepared report to a user.

Embodiments may include one or more of the following. The method may further include transmitting a request for the information. The virtual private network functions may include providing a tunnel and/or authentication. The attribute may include a tunneling characteristic (e.g., tunnel capacity, number of users actually using a tunnel, the protocol used by a tunnel). The method may further include receiving a time interval, and
preparing the report based on the received time interval.

In general, in another aspect, the invention features a method of managing a virtual private network that includes transmitting a request for tunneling data to multiple computers providing virtual private network tunnels, receiving the requested tunneling data from the multiple computers in response to the request, preparing a report based on the received information, the report being organized into a table that lists the different computers

and their corresponding tunneling data, and displaying the prepared report to a user.

In general, in another aspect, the invention features a method of monitoring a virtual private network that includes receiving information from multiple computers providing virtual private network tunnels, the information including a number of tunnels provided by each computer and a number of users configured to use the tunnels, and displaying the received information to a user.

In general, in another aspect, the invention features a method of monitoring a virtual private network that includes receiving information from multiple computers providing virtual private network tunnels, the information including usage of tunnel protocols over a period of time, and displaying the received information to a user.

In general, in another aspect, the invention features a computer program product, disposed on a computer readable medium, for managing a virtual private network. The computer program includes instructions for causing a processor to receive information describing at least one virtual private network attribute from multiple computers providing at least one virtual private network function, prepare a report by organizing the received information into a table that include the at least one virtual private network attribute received from each of the multiple computers, and display the prepared report to a user.

Advantages may include one or more of the following. The reports describing virtual private network configuration and activity eases administration of different computers providing virtual private network functions. The capacity

information enables an administrator to determine whether a particular virtual private network computer can handle tunnel requirements for additional users. The trending information also provides an administrator with a valuable snapshot of the current tunneling activity served by a particular computer.

Other advantages of the invention will become apparent in view of the following description, including the figures, and the claims.

Brief Description of the Drawings

FIG. 1 is a diagram illustrating bulk configuration of multiple extranet switches.

FIG. 2 is a diagram of tunnels provided by configured extranet switches.

FIG. 3 is a flow-chart of a process for bulk configuring multiple extranet switches.

FIG. 4 is a diagram of a switch manager exporting configuration information to multiple extranet switches.

FIGS. 5-13 are screenshots of a wizard that guides an administrator through a bulk configuration process

FIG. 14 is a diagram illustrating importing information from multiple extranet switches.

FIG. 15 is a diagram of a switch manager importing information from an extranet switch.

FIGS. 16-20 are screenshots of extranet switch reports.

FIGS. 21-31 are screenshots of a graphical user interface that enables an administrator to manage extranet switches in a virtual private network.

FIG. 32 is a screenshot of a menu of links to web-pages offered by an extranet switch.

FIGS. 33-39 are screenshots of web-pages offered by an extranet switch.

Description of the Preferred Embodiments

Introduction

An extranet switch manager provides administrators with a tool that centralizes management of different extranet switches in a virtual private network. The manager can bulk configure multiple extranet switches, prepare reports describing the extranet switches, provide convenient access to individual switch configuration mechanisms, and provide an intuitive representation of virtual private network elements. The manager offers these capabilities to an administrator via an easy to use graphical user interface (GUI). After an administrator enters IP (Internet Protocol) addresses of extranet switches in a virtual private network, the switch manager can quickly import and export data to both view the current configuration and activity of the switches and quickly alter the configuration of one or more switches.

Bulk Configuration of Multiple Extranet Switches

As shown in FIG. 1, a virtual private network 102 can include private networks 106, 110 and/or remote computers 114 that communicate over a public network 104. Each private network 106, 110 can connect to the public

network 104 via an extranet switch 100a, 100b such as a Contivity™ Extranet Switch offered by Nortel Networks. As shown, each extranet switch 100a, 100b has a private interface that communicates with a private network 106, 110 and a public interface that communicates with the public network 104. Extranet switches 100a, 100b handle virtual private network functions such as network packet tunneling and authentication. The extranet switches 100a, 100b can also enforce packet filtering rules, enforce hours of access, and perform other functions that maintain a secure virtual private network. Many of these functions may be included in a firewall or router. Hence, we use the term "extranet switch" to generically refer to a system providing these functions. As shown in FIG. 1, switch manager instructions 116 reside on a remote computer, however, the instructions 116 could reside on any computer able to communicate with the extranet switches 100a, 100b.

Each switch 100a, 110b can provide different tunneling protocols (e.g., PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunnel Protocol), and IPSec (IP Secure)), different encryption schemes, different authentication mechanisms (e.g., internal or external LDAP (Lightweight Directory Access Protocol) and RADIUS (Remote Authentication Dial-In User Service)), and different packet filtering schemes (e.g., filtering based on the direction of communication, the source and/or destination of a packet, and/or the type of TCP (Transfer Control Protocol) connection established). As shown in FIG. 1, switch manager instructions 116 enable an administrator to quickly configure multiple switches 100a, 100b to share a

set of common characteristics (e.g., the same authentication scheme and the same tunneling protocols) by transmitting the same configuration information 118a, 118b to each switch 100a, 100b.

Referring to FIG. 2, after being configured, the virtual private network 102 permits secure communication between private networks 106, 110. For example, a computer 112 on a first private network 110 can securely send network packets to a computer 108 on a second private network 106 by tunneling 120 through the public network 104. An extranet switch 100a receiving a packet prior to transmission over the public network 104 can provide a tunnel 120 by encrypting and/or encapsulating the network packet. Encryption encodes packet contents to prevent computers on the public network from reading the original contents. Encapsulation generates a new packet addressed to the extranet switch 100b at the end of the tunnel 120 and includes the original packet as the contents of the new packet. By analogy, encapsulation is like placing a mail envelope in a bigger envelope with a different mail address. Encapsulation prevents computers on the public network 104 from identifying the addresses of private network 106, 110 resources.

When the extranet switch 100b at the end of the tunnel 120 receives a packet, the extranet switch 100b can decrypt and de-encapsulate the packet for delivery to its destination 108. The second extranet switch 100b can also authenticate information received from the first extranet switch 100b to make sure a would-be intruder is not masquerading as a member of the virtual private network 102.

As shown, a switch 100a can also provide tunnels for a remote user 114 connected to the public network 104. For example, an employee can access private network 110 resources by connecting to an ISP (Internet Service Provider) and establishing a tunnel 122 with an extranet switch 100a. Again, the extranet switch 100a can authenticate the identity of the remote user 114 to prevent unauthorized access to the private network 110.

The extranet switch 100a can also connect tunnels. For example, if so configured, the switch could connect 124 tunnels 120 and 122 to enable the remote user 114 to also access resources on private network 106 via tunnels 122 and 120.

Referring to FIG. 3, switch manager instructions 116 receive 126 information specifying the configuration of multiple extranet switches. The bulk configuration information can be specified by a user, provided by a program that automatically configures switches, or copied from configuration information of a previously configured switch. After receiving 126 the configuration information, the switch manager instructions 116 transmit 128 data and/or instructions corresponding to the received configuration information to the extranet switches. Each extranet switch processes 130a, 130b the transmitted information to change its configuration in accordance with the transmitted information.

Referring to FIG. 4, an extranet switch 100a, 100b includes software and/or firmware instructions 130a, 130b that handle switch functions. Such functions can include authentication 132a, tunnel management 134a, packet

filtering 136a, etc. Each switch 100a, 100b can also include a script interface 138a that processes script commands. For example, a script command of "call omSET using ("trustedFTPenabled" "ENABLED")" configures the switch to allow processing of FTP (File Transfer Protocol) requests from trusted computers.

In one implementation, switch manager instructions 116 include instructions for a graphical user interface 144 (GUI), a script interface 140, and configuration 142 instructions that model the extranet switches and coordinate the exchange of information between the GUI 144 and the script interface 140. When a user specifies bulk configuration information via the GUI 146, the script interface 142 produces a script 118a, 118b that includes script commands for configuring the switches in accordance with the user specified information. Appendix A includes a sample configuring script. In the implementation described above, the switch manager 116 can export the configuration information 118a, 118b to extranet switches by transmitting the information 118a, 118b to a pre-determined switch directory via FTP (File Transfer Protocol). The script interface 138a, 138b on the switches 100a, 100b detect and process the script upon its arrival.

The exporting technique described above is merely illustrative and a wide variety of other techniques could be used to coordinate communication between a computer executing switch manager instructions 116 and the different extranet switches 100a, 100b. For example, the communication need not use FTP nor need the information take the form of a script.

Referring to FIG. 5, the GUI provides a wizard (e.g., Bulk Configure Extranet Switches) that enables an administrator to bulk configure multiple extranet switches by interacting with a preprogrammed series of dialogs. The dialogs query an administrator for different sets of switch characteristics. The preprogrammed set of dialogs reduces the chances an administrator will forget to configure a particular set of switch characteristics.

Referring to FIG. 6, after invoking the bulk configuration wizard, an administrator can select one or more extranet switches to bulk configure. The manager will transmit configuration information only to the selected switches.

Referring to FIG. 7, the wizard permits an administrator to configure the selected switches to provide an account to a particular administrator. Since a single administrator may be in charge of all the switches in a virtual private network, establishment of an identical administrator account on the different switches enables the administrator to quickly login to the different switches using the same id and password.

Referring to FIG. 8, each switch may be individually configured to have a unique hostname (e.g., "NOC2000"). An administrator can bulk configure different switches to have the same DNS (domain name service) domain such as "myVPN.com". By defining a common domain for multiple switches, an administrator can thereafter refer to a particular switch by combining the domain name and the hostname (e.g., "myVPN.com/NOC2000"). Primary and backup DNS servers can translate the domain and hostname to a

particular IP (Internet Protocol) address. Thus, by specifying a common domain, the administrator can identify a switch by a memorable text entry instead of a more cryptic IP address (e.g., "255.255.68.28").

Referring to FIG. 9, an administrator can configure the services offered by the switches. For example, the administrator can enable or disable different tunnel protocols (e.g., IPSec, PPTP, LT2P, and L2F). The GUI also gives the administrator the ability to enable or disable tunneling sessions initiated from within the private network served by a switch and tunneling sessions initiated from a source outside the private network (e.g., "public" tunnels).

The administrator can also enable or disable different communication protocols such as HTTP (HyperText Transfer Protocol), SNMP (Simple Network Management Protocol), FTP (File Transfer Protocol), and TELNET. Additionally, the manager gives the administrator the ability to control the types of communication allowed. For example, an administrator can enable or disable tunnels between two extranet switches (e.g., branch to branch communication), between two users tunneling to the same switch (e.g., end user to end user), and between a user and a branch office tunneling to the same switch.

Referring to FIG. 10, an administrator can bulk configure the SNMP traps reported by the switches and the host computers that will receive notification of the traps. SNMP traps allow an administrator to react to events that need attention or that might lead to problems. The switches allow the scripting of SNMP alerts so that a combination of system variables can signal an SNMP trap. The GUI permits

the administrator to not only enable or disable different types of traps, but also to provide the interval between execution of the SNMP scripts.

Referring to FIG. 11, an administrator can also configure RADIUS accounting performed by each selected switch. RADIUS is a distributed security system that uses an authentication server to verify dial-up connection attributes and authenticate connections. RADIUS accounting logs sessions with records containing detailed connection statistics. The administrator can enable and disable RADIUS accounting, configure the switches to use internal or external RADIUS servers, and specify how frequently RADIUS records are stored. By configuring the switches in a virtual private network to use the same RADIUS accounting methods, switch usage and access can be easily compared between the different switches.

Referring to FIG. 12, if enabled, an administrator can bulk configure the type of RADIUS authentication performed by the switches. For example, as shown, the switches can offer AXENT (AXENT OmniGuard/Defender), SecurID (Security Dynamics SecurID), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol encrypted), CHAP (Challenge Handshake Authentication Protocol), and/or PAP (Password Authentication Protocol) authentication.

The administrator can also define a primary RADIUS server and one or more alternate servers. The primary server receives all RADIUS authentication inquiries unless it is out of service. In the event that the Primary Server is unreachable, the Switch will query the alternate RADIUS servers. By bulk configuring the servers used to provide

RADIUS authentication, administrators can quickly route all RADIUS authentication requests to the same collection of RADIUS servers.

Referring to FIG. 13, switches may use LDAP authentication in addition to or in lieu of RADIUS authentication. An external LDAP Server such as the Netscape Directory Server can store remote access profiles. The switch queries the LDAP Server for access profile information when a user attempts to establish a tunnel connection. The Master LDAP Server is the primary server to process queries. Should the Master server become unavailable, the switch attempts to initiate a connection with the Slave servers. Bulk configuring different switches to use the same LDAP servers both eases the burden of switch management on the administrator and reduces the likelihood the administrator will inadvertently specify a different LDAP hierarchy on different switches.

After completing the bulk configuration wizard, the manager stores the specified configuration information, but does not transmit the information until the administrator specifically exports the configuration data. This provides administrators with a safeguard against accidentally bulk configuring the switches with unintended characteristics.

Reporting Capabilities

Referring to FIG. 14, in addition to configuring multiple extranet switches 100a, 100b, switch manager instructions 116 can also produce reports describing the extranet switches 100a, 100b in a virtual private network 102. As shown, the extranet switches 100a, 100b can

transmit configuration, capacity, and activity information for inclusion in a report.

Referring to FIG. 15, switch manager instructions 116 can transmit a script 152a, 152b that includes script commands requesting current switch 100a, 100b information. For example, a script command of "call omGET using ("security.trustedFTPenabled")" requests information describing whether an extranet switch 100a, 100b is currently configured to accept FTP (File Transfer Protocol) requests from a trusted computer. Appendix B includes a sample script requesting information from a Contivity™ switch.

The switch 100a, 100b script interface 138a, 138b processes the script commands 128 and produces a file 150a, 150b including the requested information. The script interface 138a, 138b on the switch 100a, 100b can store the file in a pre-determined directory. The switch manager instructions 116 can then use FTP to retrieve the information 150a, 150b.

Again, a wide variety of other techniques could enable the switches 100a, 100b to communicate with the switch manager instructions 116. Additionally, instead of the request/response model described above, the switches 100a, 100b could schedule periodic execution of a script and/or periodic transmission of the switch information 150a, 150b.

Referring to FIG. 16, the switch manager GUI can provide a menu of different reports that can be produced for selected extranet switches. The manager prepares the report

by analyzing and/or including data imported from the different extranet switches.

Referring to FIG. 17, a first report can display different static attributes of the selected switches such as DNS details.

Referring to FIG. 18, a security report displays the security configurations of the selected switches such as the enabling/disabling of different tunneling and communication protocols. The security report can also list changes made to the selected switch configurations when such changes occurred (not shown). The report can also include information summarizing failed access attempts to the switches (not shown). This report enables an administrator to quickly view the different security configurations and any troublesome security statistics.

Referring to FIG. 19, a capacity report shows the current total capacity of tunnels that selected switches can provide and the total number of subscribers and/or users configured to use the switch. This report provides a simple but useful gauge of tunnel capacity. Based on the capacity report, an administrator can decide whether to add more subscribers to an available tunnel pool or to increase the size of tunnel pool, for example, by upgrading or adding an extranet switch.

Referring to FIG. 20, a trending report displays the number of tunnels for each tunnel technology provided by the different extranet switches over a user-specified amount of time. The report allows subscribers to select any number of currently defined switches or services.

Custom Views

Referring to FIG. 21, the switch manager GUI eases administration of a virtual private network extranet switches by collecting information about the entire network in a single display. As shown, the switch manager GUI displays configuration information imported from one or more extranet switches (e.g., via the import mechanism described in conjunction with FIG. 15). The GUI uses a split screen display that includes a navigation pane 200 listing different virtual private network switches 202, subscribers 204, and other information such as periodic scheduling 206 of management functions and scripts 208 that can perform these functions. As shown, the listing uses a hierarchical tree to display the virtual private network elements. An administrator can view a listed element in more detail by expanding the tree (e.g., clicking on the "-" or "+" next to an element). The tree display enables an administrator to quickly find, add, remove, and configure different virtual private network extranet switches.

As shown, the display also provides a tabbed dialog control 210 that provides more information and management options for a virtual private network element currently selected in the navigation pane 200 (e.g., "Configuration Data" 212). The control 210 includes dialogs for adding new elements to the tree from a palette 214 of elements, for viewing and altering properties 216 of a selected element, for a list of wizards 218 that perform tasks frequently used with a selected element, and a list of network links 222 that enable an administrator to manually configure an individual extranet switch. By providing management options

corresponding to an element selected in the navigation pane 200, the GUI presents only a relevant subset of a wide variety of different management features at a given moment.

Referring to FIGS. 22-26, the GUI enables an administrator to quickly view and modify the configuration of any particular switch in the virtual private network from within a single application. For example, as shown, an administrator can quickly add a new subscriber 226 to the virtual private network. Briefly, a subscriber is any entity that uses a virtual private network service (e.g., a tunnel protocol). For example, service providers typically use the same extranet switch to provide virtual private network services to different organizations. In this case, each organization could be considered a subscriber. Subscribers can also be individual users.

As shown in FIG. 22, after selecting the "Configuration Data" element 212, a palette tab presents different elements that can be added to the selected virtual private network element 212. A new subscriber 226 can be added by dragging-and-dropping the subscriber 224 palette tool onto the "Configuration Data" element 212. As shown in FIG. 23, the administrator can rename the new subscriber 226. As shown in FIG. 24, by selecting the new subscriber 226, selecting the "palette" tab 214, and dragging a "VPN Service" 228 (e.g., a tunnel) from the palette onto the new subscriber 226, the administrator can also configure a switch or switches to offer a particular tunneling protocol.

As shown in FIG. 25, the administrator can name the tunnel, define the tunneling technology used by the tunnel

(e.g., L2TP), and enter the tunnel starting and ending points which, as shown, are extranet switches.

As shown in FIG. 26, after configuring different subscribers and switches, the GUI provides an administrator with a variety of different methods of looking at a virtual private network. For example, as shown, by expanding a subscriber 232 an administrator can quickly see shortcuts to the extranet switches 236, 238 offering tunnels for subscriber use. Alternatively, as shown in FIG. 27, the administrator can view the tunneling technologies offered by a particular switch 240 by using the navigation pane 200 to select the switch's tunnel element 242. The properties dialog 244 displays the configuration of the different tunneling technologies.

The different presentations of the data (e.g., subscriber based and switch based) described above enable the administrator to both ensure that subscribers are adequately served and that individual switches are configured as desired.

Referring to FIGS. 28-29, the process described above (i.e., selecting an element from the tree and using the tabbed dialog to view and modify the element's characteristics) can be used to configure a variety of virtual private network characteristics. For example, by selecting a switch 240 from the navigation pane 200, the administrator can view and modify the switch's 240 characteristics. As shown in FIG. 28, an administrator can add RADIUS Authentication 244 to a switch 240 by dragging-and-dropping the RADIUS Authentication Server palette selection 242 onto the selected switch 240. As

shown in FIG. 29, the administrator can then set different RADIUS authentication settings for the switch 244. An administrator can use a similar technique to add and/or configure SNMP (Simple Network Management Protocol) settings, switch interfaces to private and/or public networks, Ethernet settings, IPX (Internetwork Packet Exchange) settings, and other extranet switch features displayed in the switch palette. Appendix C includes screenshots of the different palette elements and their properties that can be used to configure an extranet switch.

The alterations to the switches, for example, adding RADIUS authentication to a switch, while immediately represented to the administrator, is not exported until explicitly requested by the administrator. Again, this gives the administrator a chance to avoid unintended modifications.

Referring to FIGS. 30-31, beyond viewing and modifying switch characteristics, an administrator can use the GUI to organize information for easy access and identification of different elements. For example, as shown in FIG. 30, an administrator can drag a folder 250 from the palette onto an element. The administrator can rename the dragged folder 252 (e.g., to "Subscribers") and drag-and-drop different subscribers into the folder 252. As shown in FIG. 31, a similar technique enables an administrator to organize different switches into different groupings such as switches using LDAP 254 for authentication and switches using RADIUS 256.

Integrated Access to a Switch's Configuration Mechanisms

As previously described, an extranet switch such as the Contivity™ switch can include a web-server and different network pages (e.g., HTML (HyperText Markup Language) documents) that enable an administrator to individually configure an extranet switch. By navigating to a switch web-server, an administrator can view and/or modify a switch's configuration.

Referring to FIG. 32, the GUI can present a menu 260 of network links (e.g., link 268) to web-pages offered by a selected extranet switch 270. As shown, the menu 260 includes a description of the link 272 and a corresponding URL (Universal Resource Locator) identifying a web-page offered by a switch. As shown, the URL includes designation of a communication protocol (e.g., HTTP (HyperText Transfer Protocol) 262, an IP address 264, and the location of a particular page at the specified IP address 268. When a user selects a link from the menu 260, the switch manager can transmit an HTTP request for the selected URL. Alternately, the switch manager can instantiate or call a network browser and pass the selected URL. The GUI prepares each URL in the menu 260 by prepending a switch's IP address 264 to a predefined set of web-page locations 266.

By providing the link menu in conjunction with the navigation pane 200, administrators can quickly access a desired page on any particular switch and can also quickly access the same page (e.g., the users page) on a variety of different switches, one after another. Additionally, the menu 260 obviates the need to remember the different extranet switch URLs or expend the time needed to navigate

through any menu provided by the switch itself which necessitates potentially long waits for information to be transmitted to the switch manager.

As shown, the web-pages include pages that control how a switch handles users (FIG. 33), branch offices (FIG. 34), packet filters (FIG. 35), groups of users (FIG. 36), access hours (FIG. 37), and other information such as a menu that tailors a web-based configuration session (FIG. 39). Descriptions of the functions of these different web-pages is described in the New Oak Communications Extranet Access Switch Administrators Guide, pages 82-138 of which are incorporated by reference herein.

Other Embodiments

The embodiments described above should not be considered limiting. For example, one of skill in the art could quickly construct a switch manager that perform the functions described above using different GUI controls or a different arrangement of GUI controls.

Additionally, the techniques described here are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing environment. The techniques may be implemented in hardware or software, or a combination of the two. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code is applied to data

entered using the input device to perform the functions described and to generate output information. The output information is applied to one or more output devices.

Each program is preferably implemented in a high level procedural or object oriented programming language to communicate with a computer system. however, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

Each such computer program is preferable stored on a storage medium or device (e.g., CD-ROM, hard disk or magnetic diskette) that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described in this document. The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

Other embodiments are within the scope of the following claims.

What is claimed is:

1. A method of managing a virtual private network, the method comprising:

receiving information describing at least one virtual private network attribute from multiple computers providing at least one virtual private network function;

preparing a report by organizing the received information into a table that lists each of the multiple computers and the corresponding virtual private network attribute received from each of the multiple computers; and

displaying the prepared report to a user.

2. The method of claim 1, further comprising transmitting a request for the information.

3. The method of claim 1, wherein the virtual private network function comprises providing at least one tunnel.

4. The method of claim 1, wherein the virtual private network function comprises authentication.

5. The method of claim 1, wherein the attribute comprises at least one tunneling characteristic.

6. The method of claim 5, wherein the tunneling characteristic comprises the tunnel capacity of the computer.

7. The method of claim 5, wherein the tunneling characteristic comprises a number of users using a tunnel provided by a computer.

8. The method of claim 5, wherein the tunneling characteristic comprises a tunneling protocol.

9. The method of claim 1, further comprising receiving a time interval, and

wherein the preparing a reports comprises preparing a report based on the received time interval.

10. A method of managing a virtual private network, the method comprising:

transmitting a request for tunneling data to multiple computers providing virtual private network tunnels;

receiving the requested tunneling data from the multiple computers in response to the request;

preparing a report based on the received information, the report being organized into a table that lists the different computers and their corresponding tunneling data; and

displaying the prepared report to a user.

11. A method of monitoring a virtual private network, the method comprising:

receiving information from multiple computers providing virtual private network tunnels, the information

including a number of tunnels provided by each computer and a number of users configured to use the tunnels; and

displaying the received information to a user.

12. A method of monitoring a virtual private network, the method comprising:

receiving information from multiple computers providing virtual private network tunnels, the information including usage of tunnel protocols over a period of time; and

displaying the received information to a user.

13. A computer program product, disposed on a computer readable medium, for managing a virtual private network, the computer program including instructions for causing a processor to:

receive information describing at least one virtual private network attribute from multiple computers providing at least one virtual private network function;

prepare a report by organizing the received information into a table that include the at least one virtual private network attribute received from each of the multiple computers; and

display the prepared report to a user.

14. The computer program product of claim 13, further comprising instructions for causing the processor to transmit a request for the information.

15. The computer program product of claim 13, wherein the virtual private network function comprises providing at least one tunnel.

16. The computer program product of claim 13, wherein the virtual private network function comprises authentication.

17. The computer program product of claim 13, wherein the attribute comprises at least one tunneling characteristic.

18. The computer program product of claim 17, wherein the tunneling characteristic comprises the tunnel capacity of the computer.

19. The computer program product of claim 17, wherein the tunneling characteristic comprises a number of users using a tunnel provided by a computer.

20. The computer program product of claim 17, wherein the tunneling characteristic comprises tunneling protocol.

364393.B11

Abstract

Managing a virtual private network includes receiving information describing at least one virtual private network attribute from multiple computers providing at least one virtual private network function, preparing a report by organizing the received information into a table that lists each of the multiple computers and the corresponding virtual private network attribute received from each of the multiple computers, and displaying the prepared report to a user.

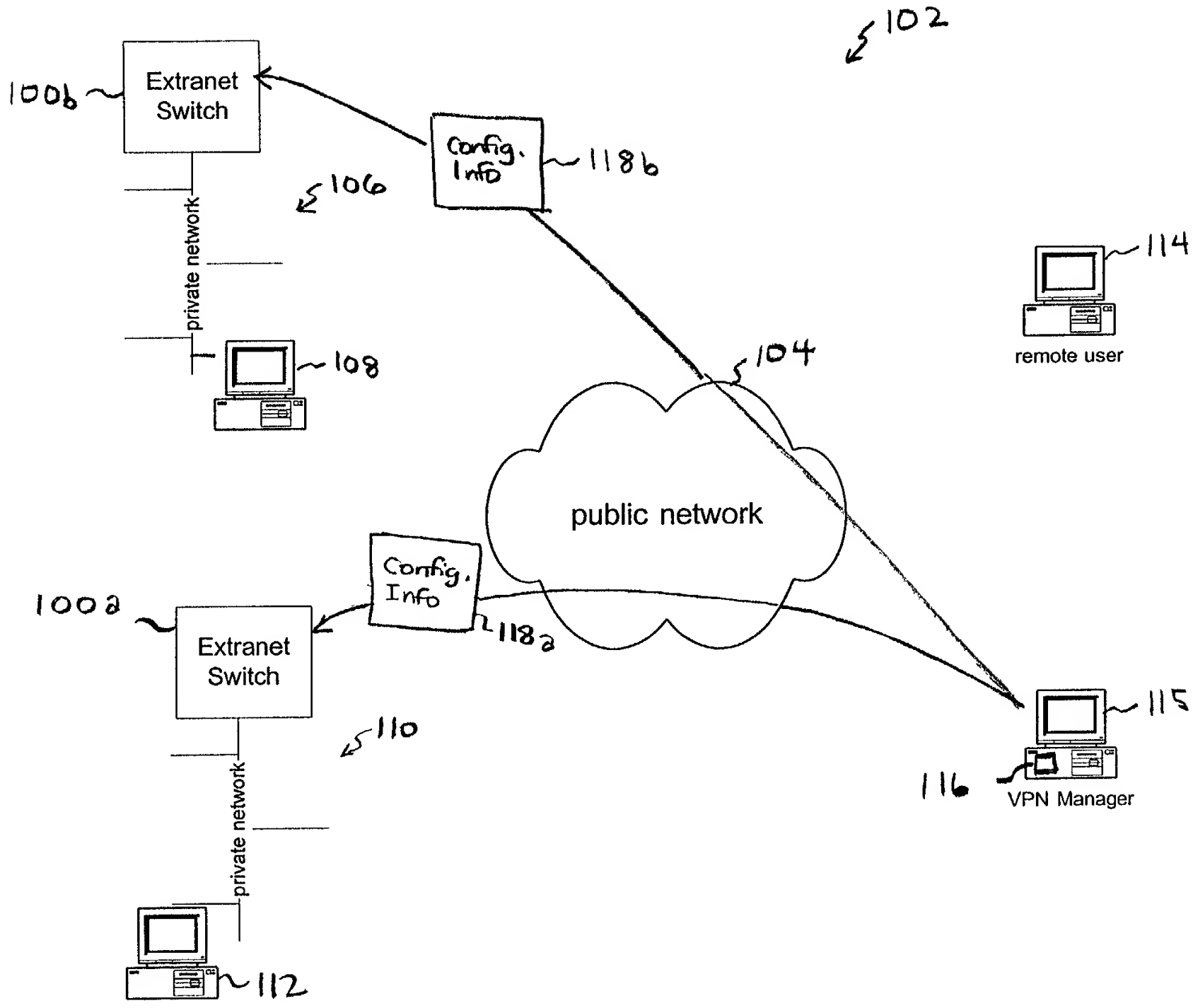
102
Extranet Switch
100b
Config. Info
118b
106
private network
108
104
public network
remote user
114
Config. Info
100a
Extranet Switch
118a
110
private network
112
115
116
VPN Manager

FIG. 1

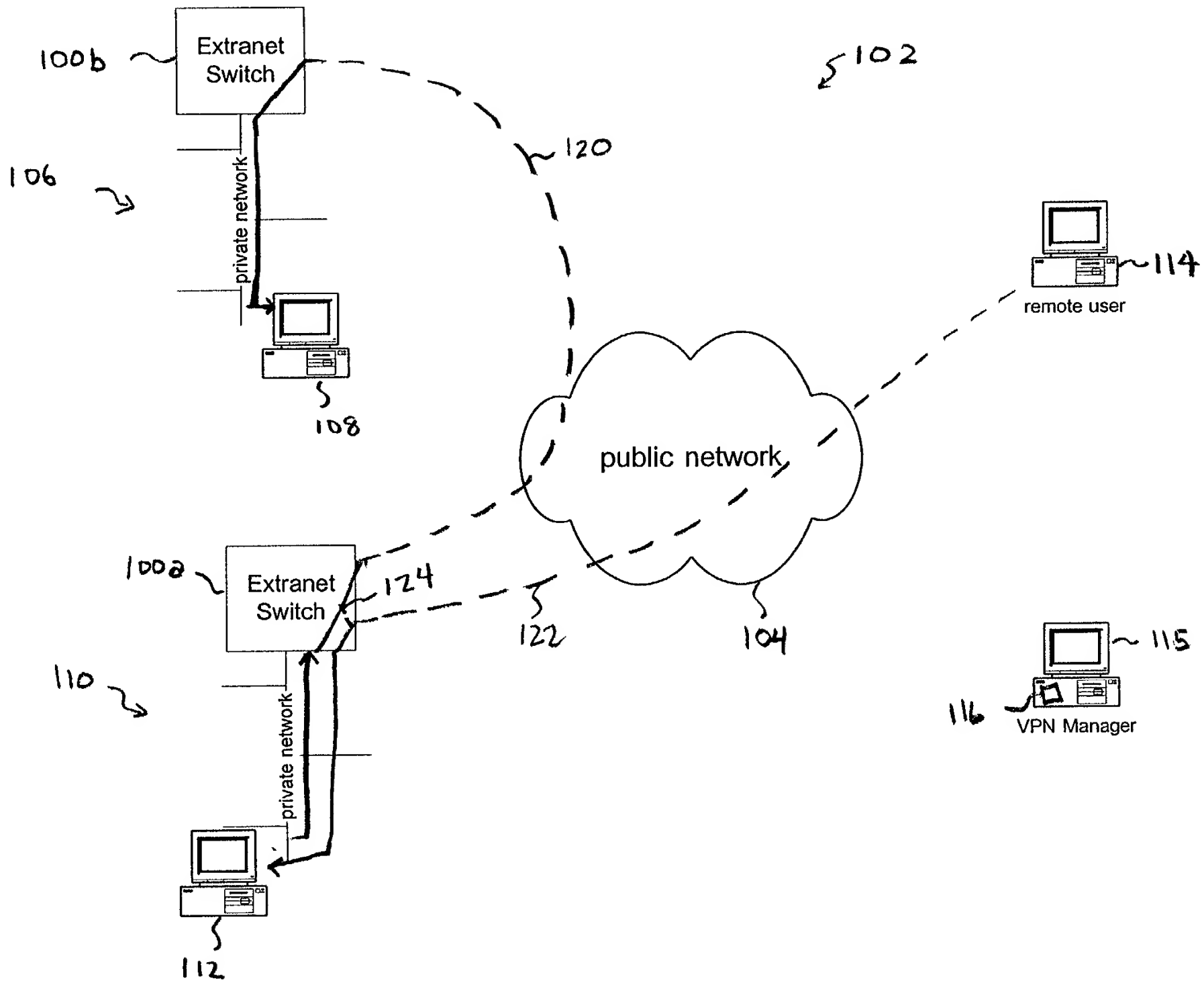
100b
Extranet Switch
102
120
106
private network
114
remote user
108
public network
100a
Extranet Switch
124
122
104
110
private network
115
116
VPN Manager
112

FIG. 2

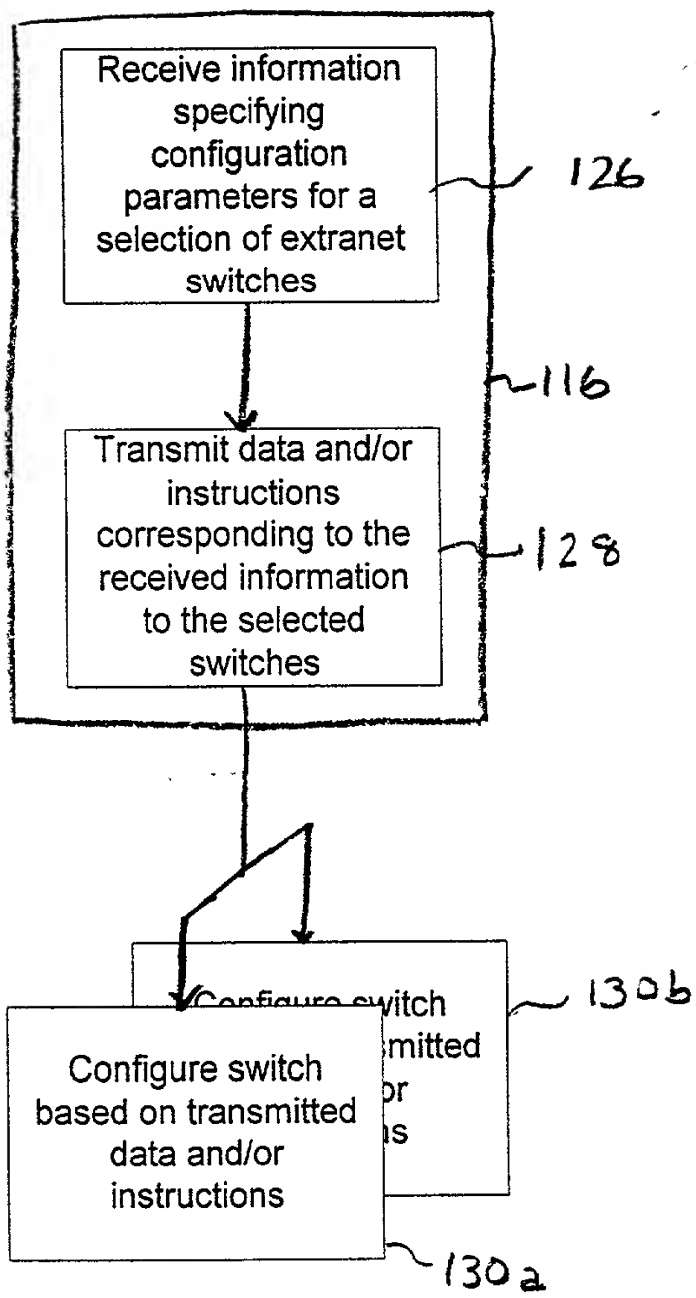
Receive information specifying configuration parameters for a selection of extranet switches
126
116
Transmit data and/or instructions corresponding to the received information to the selected switches
128
130b
Configure switch based on transmitted data and/or instructions
130a

FIG. 3

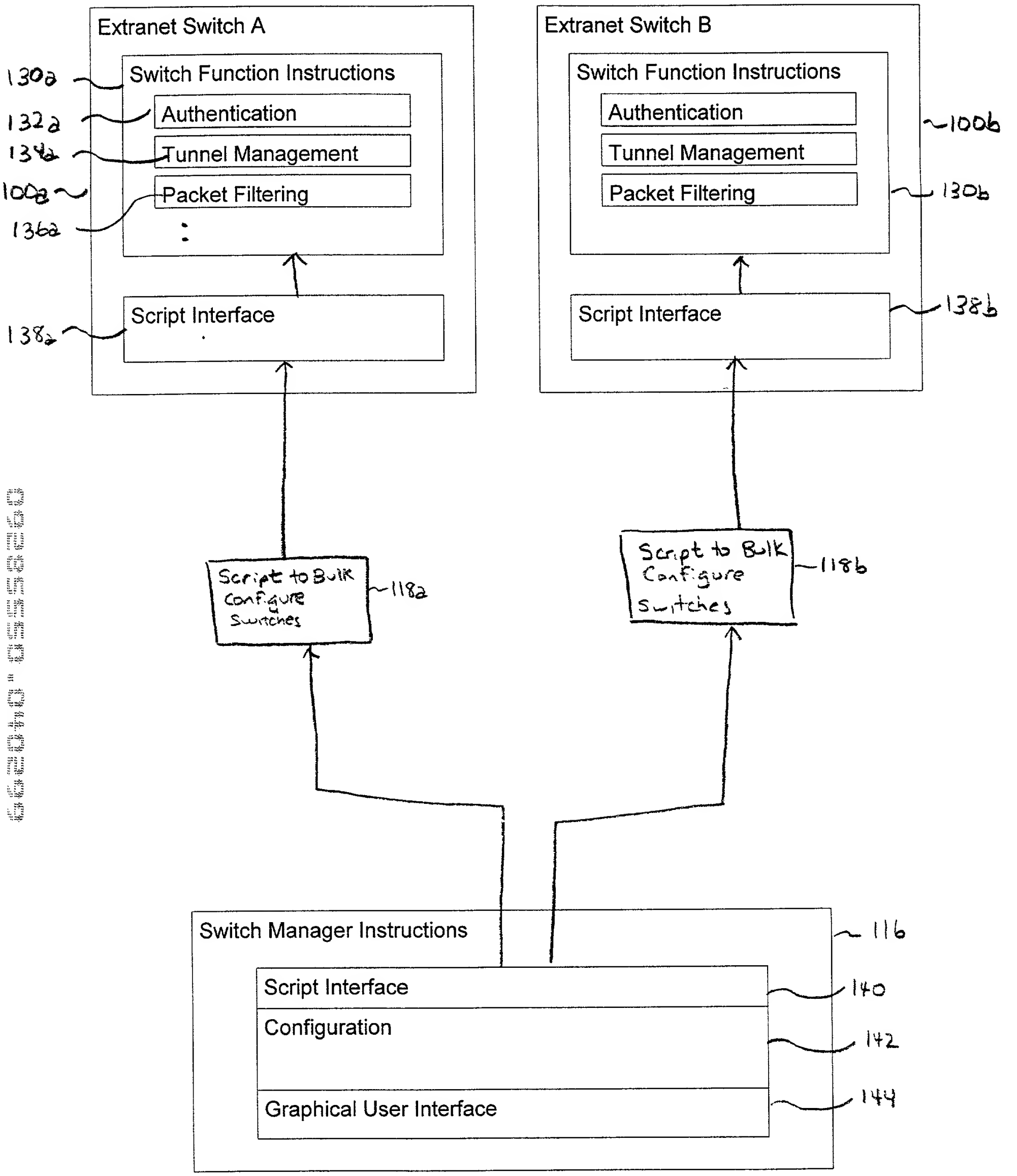
Extranet Switch A
Switch Function Instructions
Authentication
Tunnel Management
Packet Filtering
Script Interface
130a
132a
134a
100a
136a
138a
Extranet Switch B
Switch Function Instructions
Authentication
Tunnel Management
Packet Filtering
Script Interface
100b
130b
138b
Script to Bulk Configure Switches
118a
Script to Bulk Configure Switches
118b
Switch Manager Instructions
116
Script Interface
140
Configuration
142
Graphical User Interface
144

FIG. 4

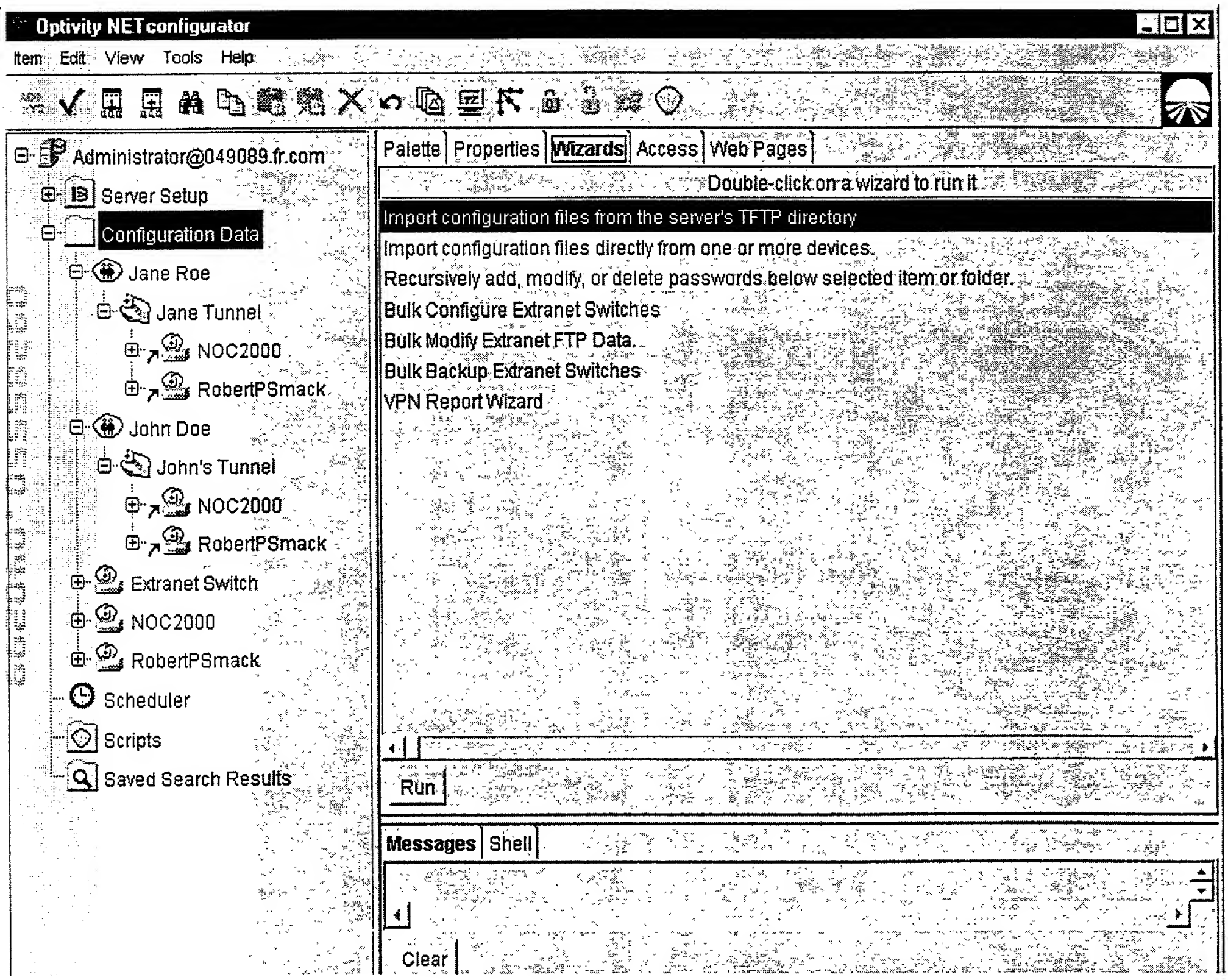
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Jane Roe
Jane Tunnel
NOC2000
RobertPSmack
John Doe
John's Tunnel
NOC2000
RobertPSmack
Extranet Switch
NOC2000
RobertPSmack
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Double-click on a wizard to run it
Import configuration files from the server's TFTP directory
Import configuration files directly from one or more devices.
Recursively add, modify, or delete passwords below selected item or folder.
Bulk Configure Extranet Switches
Bulk Modify Extranet FTP Data
Bulk Backup Extranet Switches
VPN Report Wizard
Run
Messages Shell
Clear

FIG 5

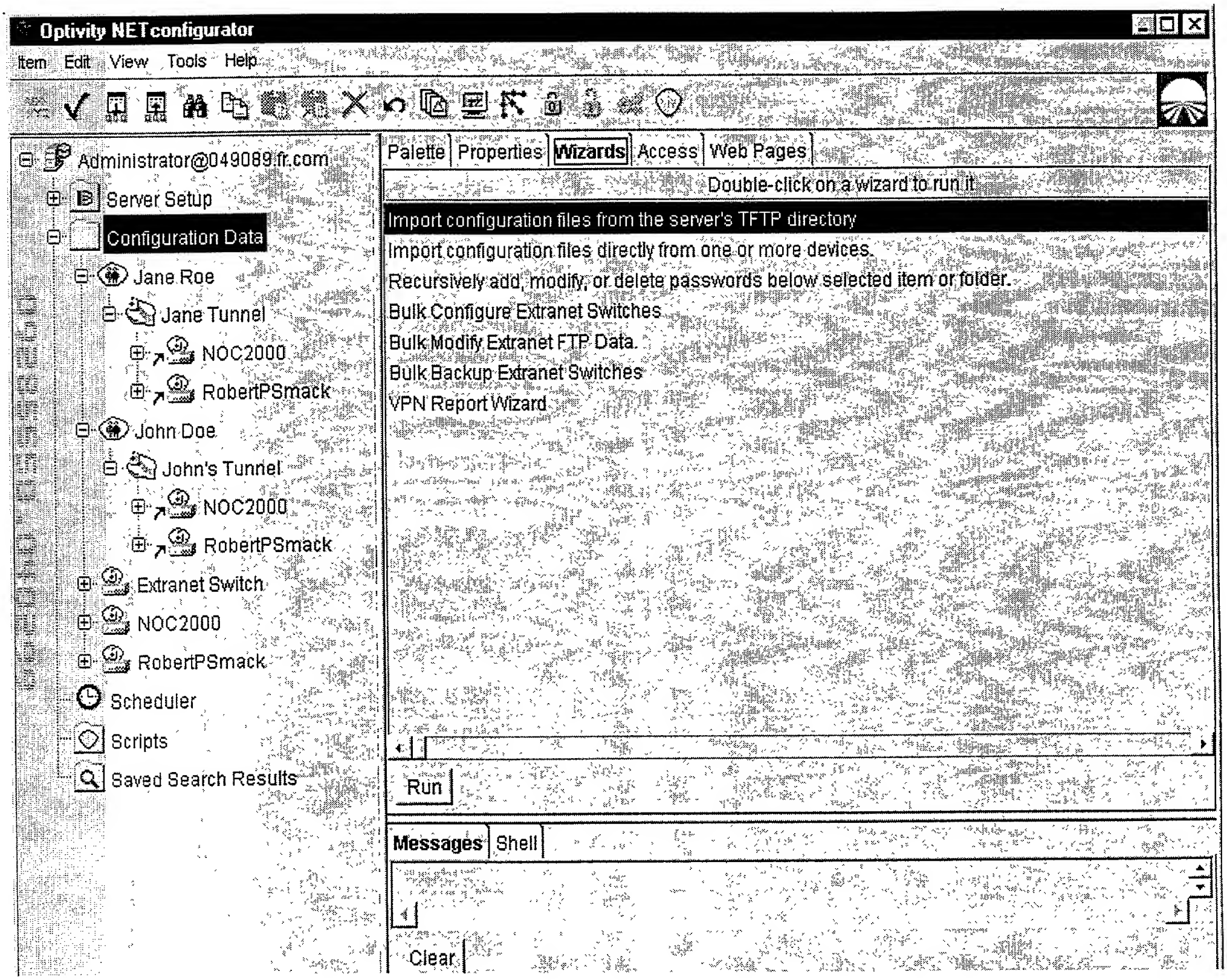
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Jane Roe
Jane Tunnel
NOC2000
RobertPSmack
John Doe
John's Tunnel
NOC2000
RobertPSmack
Extranet Switch
NOC2000
RobertPSmack
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Double-click on a wizard to run it
Import configuration files from the server's TFTP directory
Import configuration files directly from one or more devices.
Recursively add, modify, or delete passwords below selected item or folder.
Bulk Configure Extranet Switches
Bulk Modify Extranet FTP Data.
Bulk Backup Extranet Switches
VPN Report Wizard
Run
Messages Shell
Clear

Fig 5

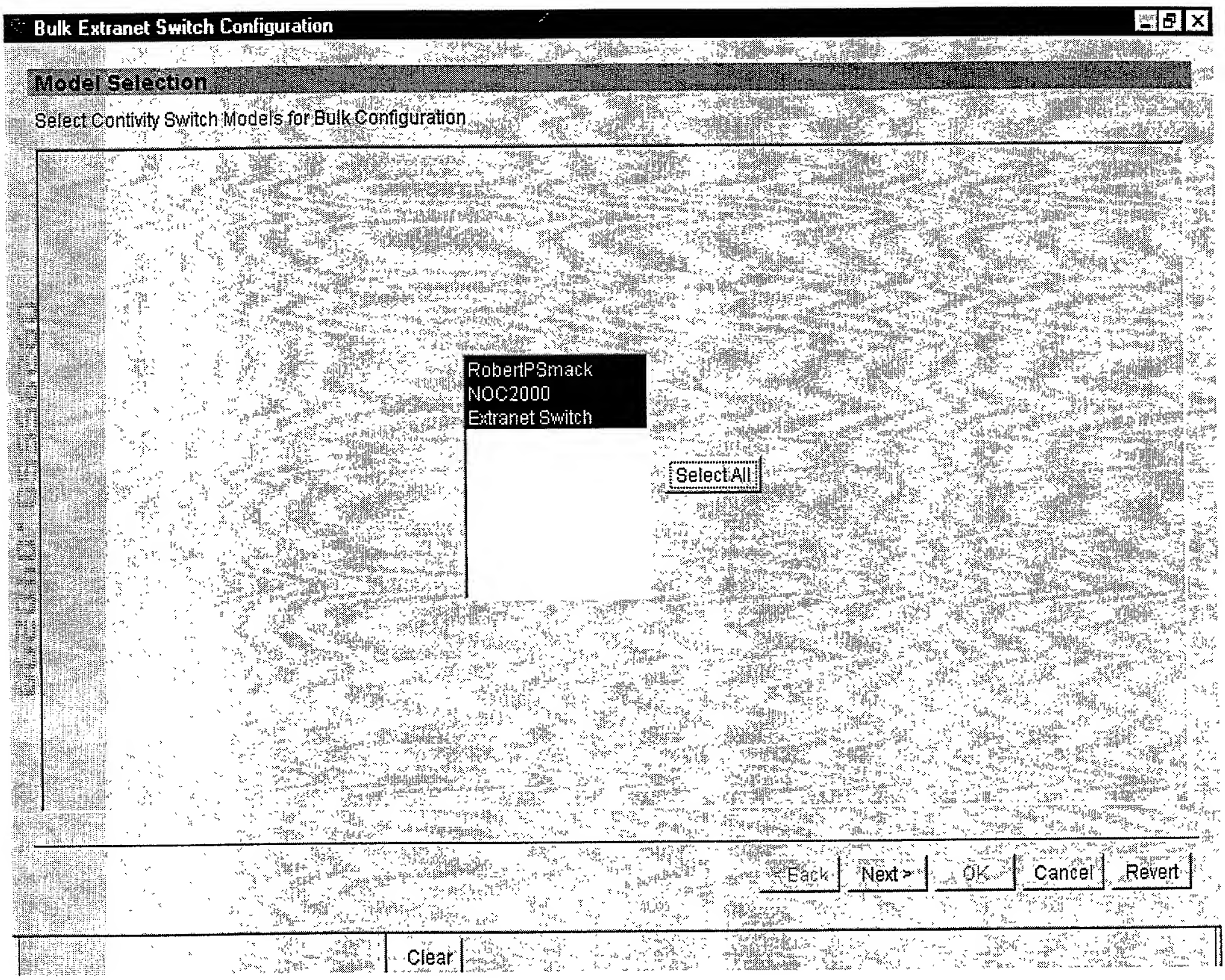
Bulk Extranet Switch Configuration
Model Selection
Select Contivity Switch Models for Bulk Configuration
RobertPSmack
NOC2000
Extranet Switch
Select All
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 6

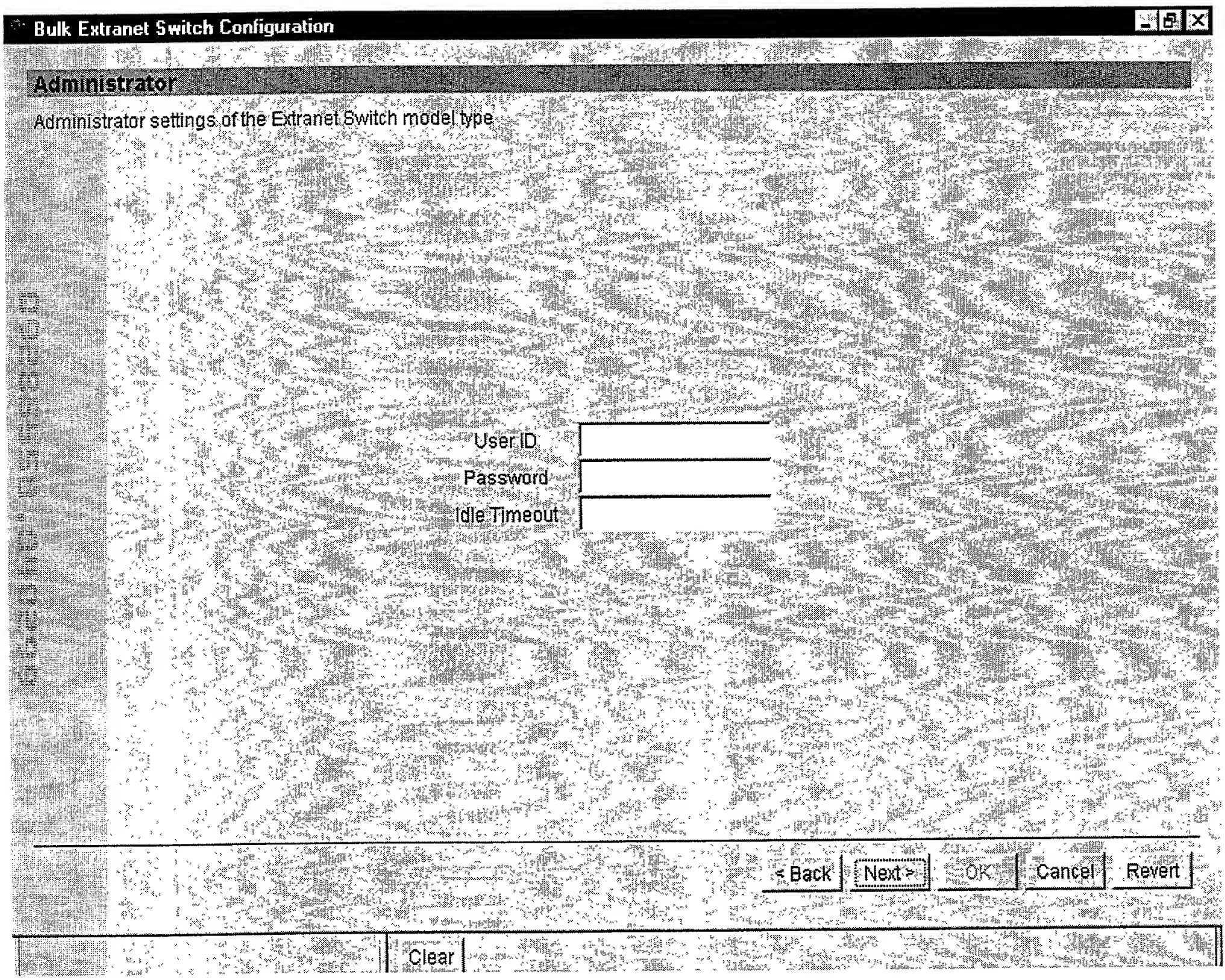
Bulk Extranet Switch Configuration
Administrator
Administrator settings of the Extranet Switch model type
User ID
Password
Idle Timeout
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 7

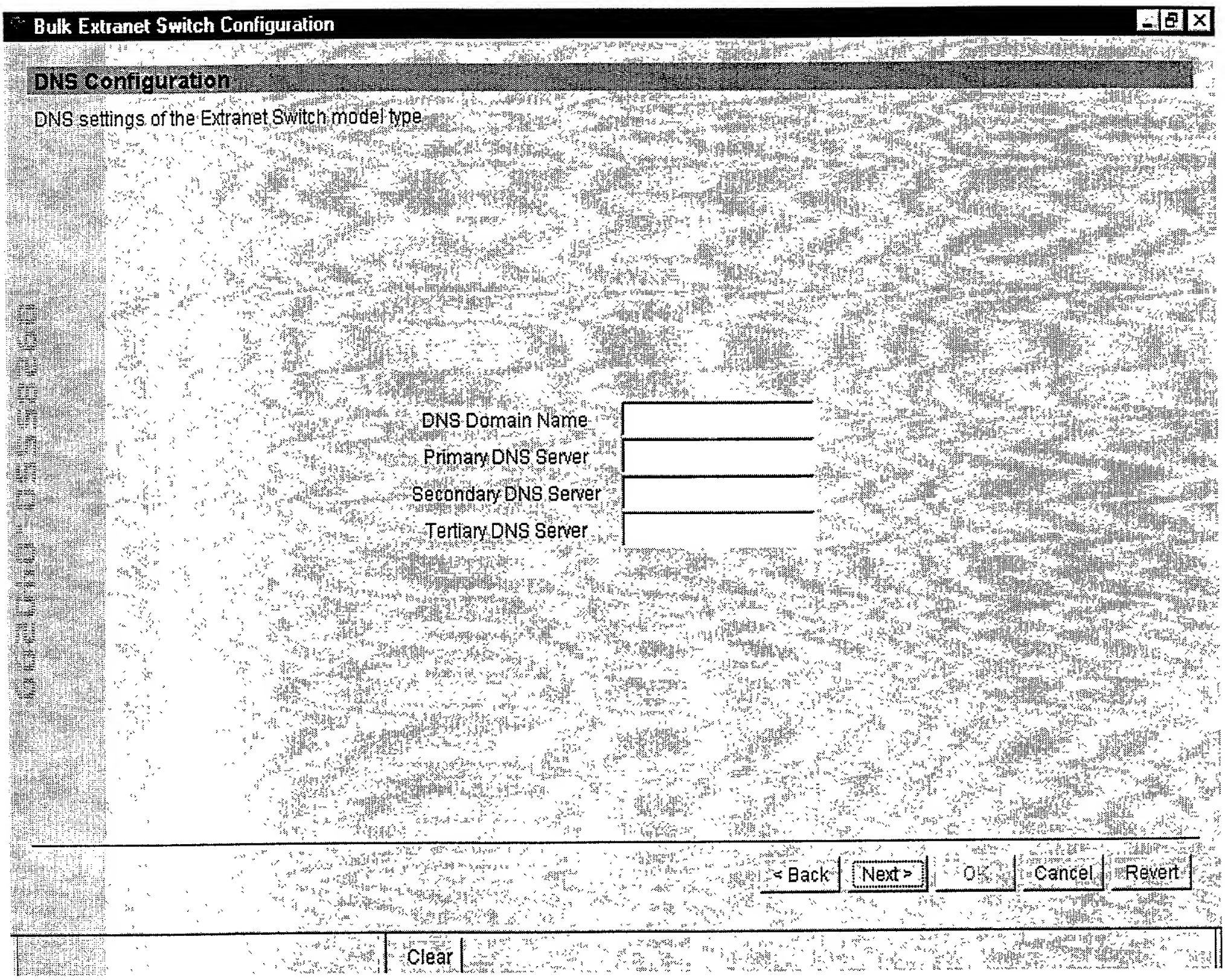
Bulk Extranet Switch Configuration
DNS Configuration
DNS settings of the Extranet Switch model type
DNS Domain Name
Primary DNS Server
Secondary DNS Server
Tertiary DNS Server
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 8

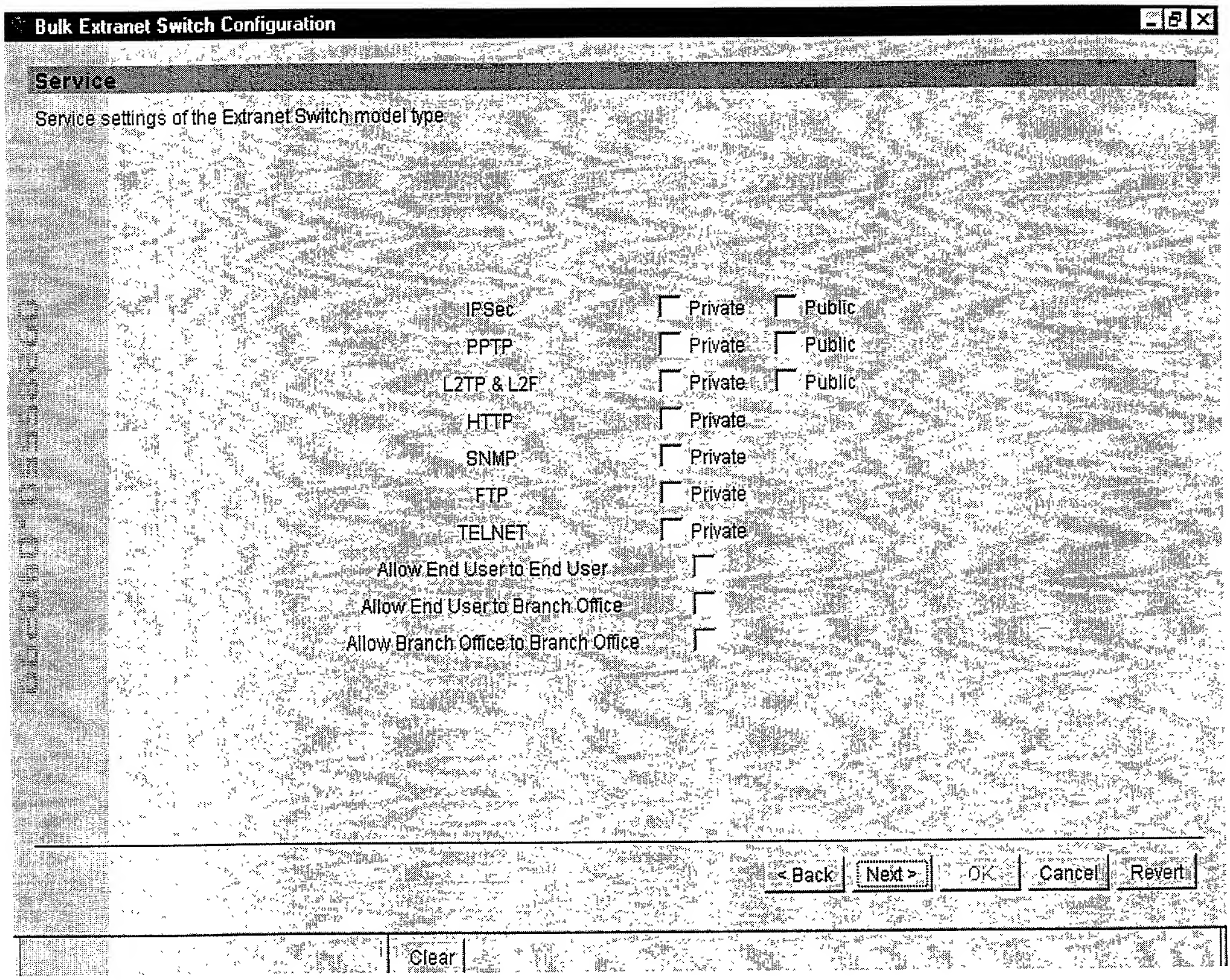
Bulk Extranet Switch Configuration
Service
Service settings of the Extranet Switch model type
IPSec
Private
Public
PPTP
Private
Public
L2TP & L2F
Private
Public
HTTP
Private
SNMP
Private
FTP
Private
TELNET
Private
Allow End User to End User
Allow End User to Branch Office
Allow Branch Office to Branch Office
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 9

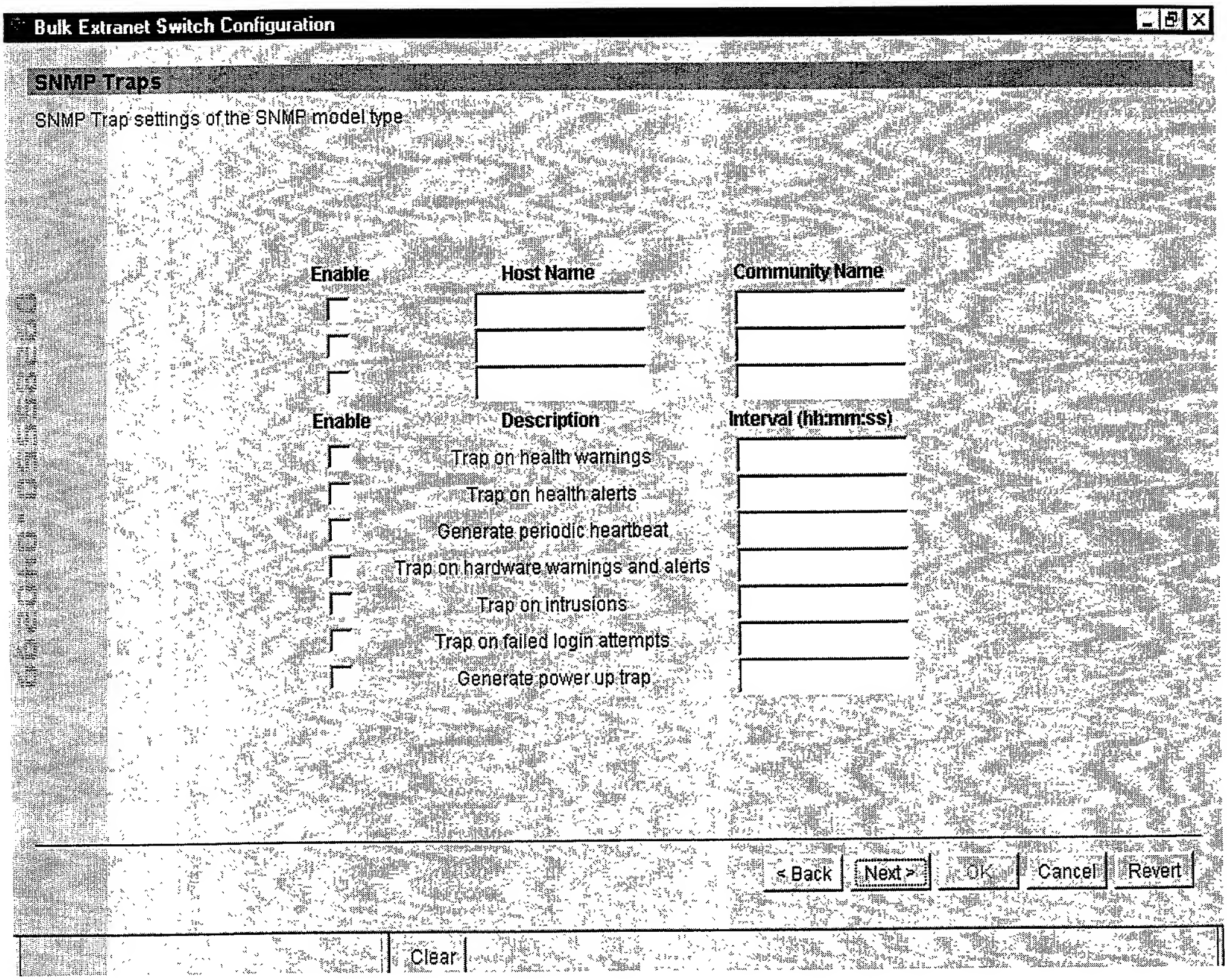
Bulk Extranet Switch Configuration
SNMP Traps
SNMP Trap settings of the SNMP model type
Enable
Host Name
Community Name
Enable
Description
Interval (hh:mm:ss)
Trap on health warnings
Trap on health alerts
Generate periodic heartbeat
Trap on hardware warnings and alerts
Trap on intrusions
Trap on failed login attempts
Generate power up trap
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 10

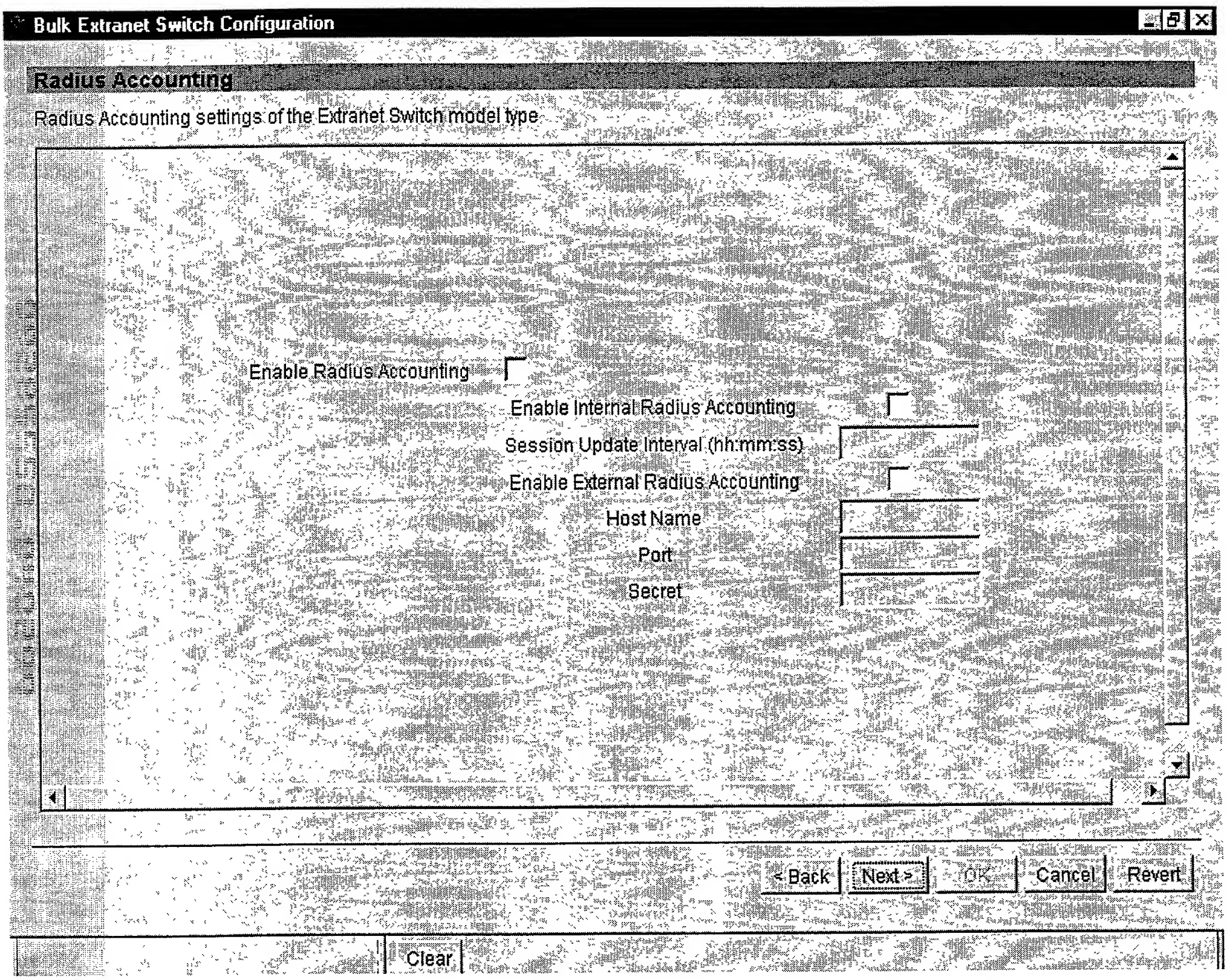
Bulk Extranet Switch Configuration
Radius Accounting
Radius Accounting settings of the Extranet Switch model type
Enable Radius Accounting
Enable Internal Radius Accounting
Session Update Interval (hh:mm:ss)
Enable External Radius Accounting
Host Name
Port
Secret
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 11

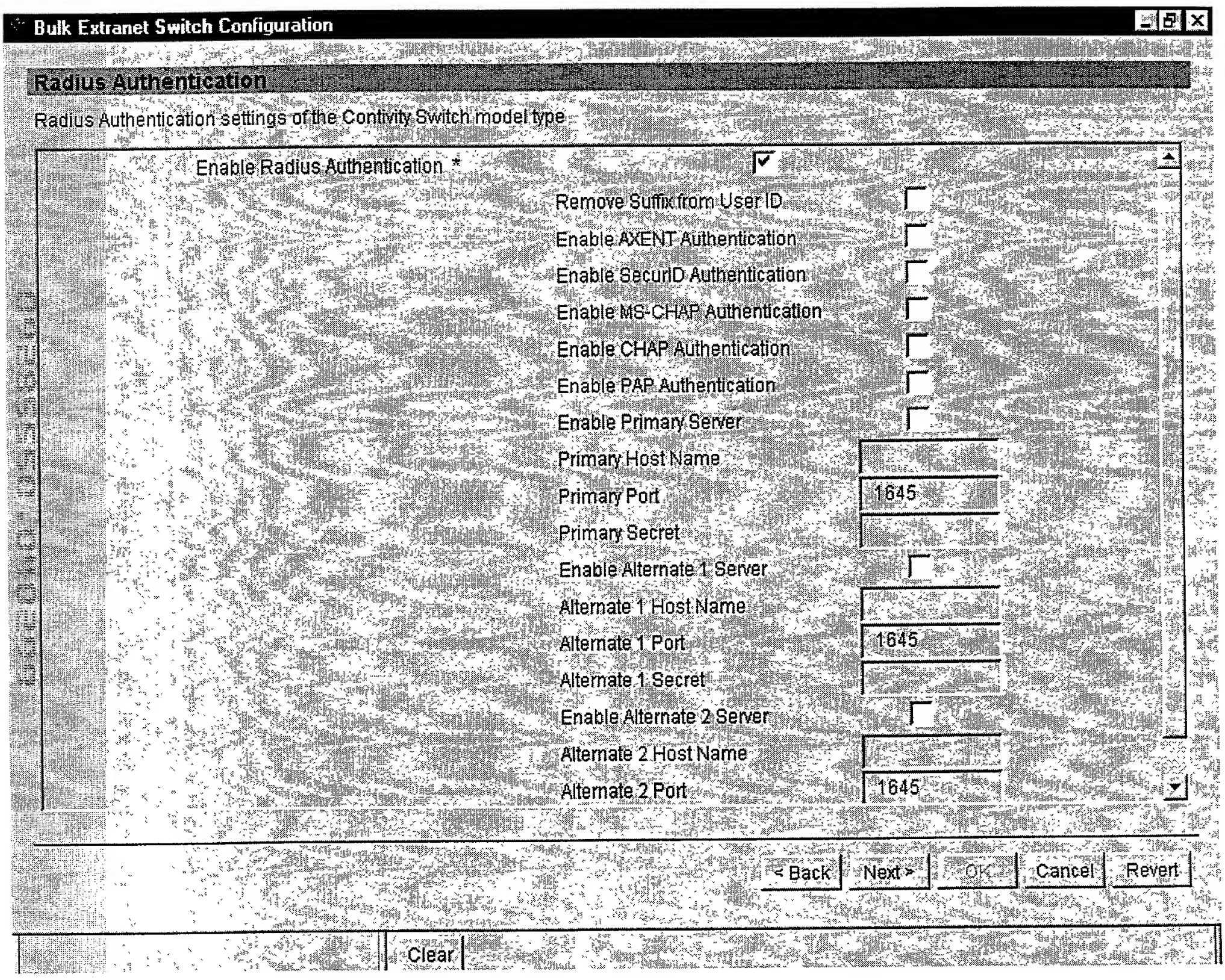
Bulk Extranet Switch Configuration
Radius Authentication
Radius Authentication settings of the Contivity Switch model type
Enable Radius Authentication *
Remove Suffix from User ID
Enable AXENT Authentication
Enable SecurID Authentication
Enable MS-CHAP Authentication
Enable CHAP Authentication
Enable PAP Authentication
Enable Primary Server
Primary Host Name
Primary Port
1645
Primary Secret
Enable Alternate 1 Server
Alternate 1 Host Name
Alternate 1 Port
1645
Alternate 1 Secret
Enable Alternate 2 Server
Alternate 2 Host Name
Alternate 2 Port
1645
< Back
Next >
OK
Cancel
Revert
Clear

FIG. 12

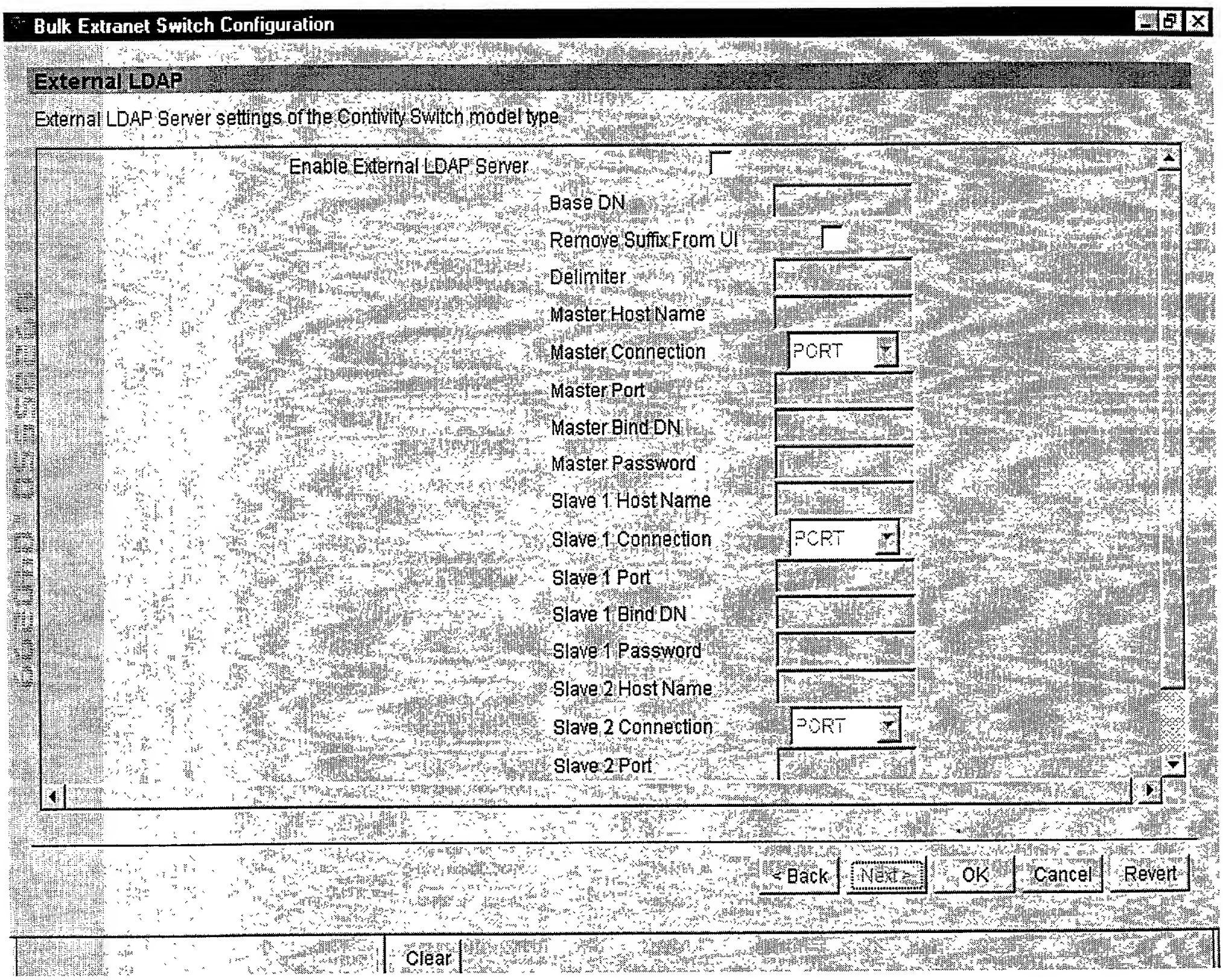
Bulk Extranet Switch Configuration
External LDAP
External LDAP Server settings of the Contivity Switch model type
Enable External LDAP Server
Base DN
Remove Suffix From UI
Delimiter
Master Host Name
Master Connection
PORT
Master Port
Master Bind DN
Master Password
Slave 1 Host Name
Slave 1 Connection
PORT
Slave 1 Port
Slave 1 Bind DN
Slave 1 Password
Slave 2 Host Name
Slave 2 Connection
PORT
Slave 2 Port
< Back
Next >
OK
Cancel
Revert
Clear

FIG.13

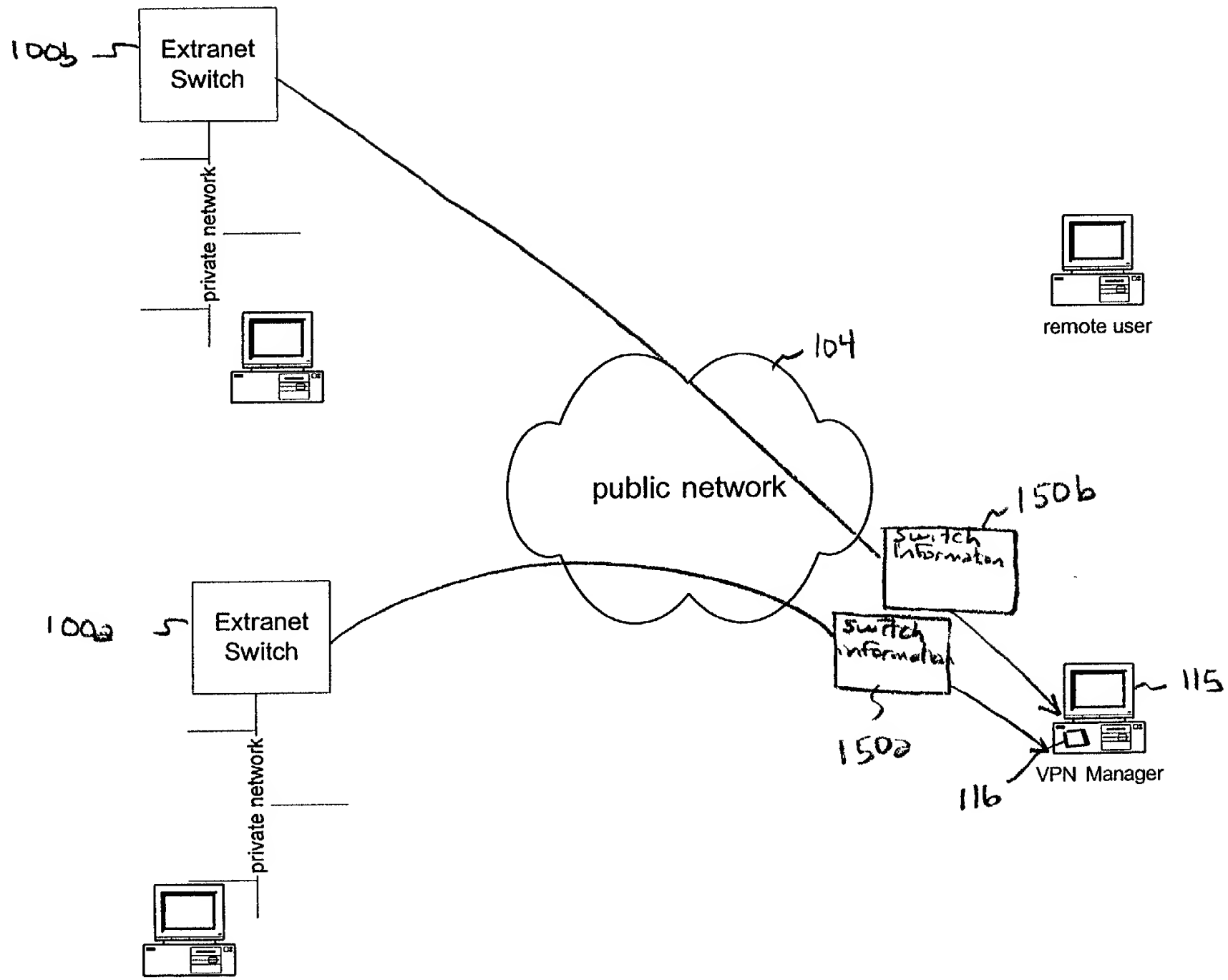
100b
Extranet Switch
private network
104
public network
remote user
150b
Switch Information
Switch Information
150a
115
VPN Manager
116
100a
Extranet Switch
private network

FIG. 14

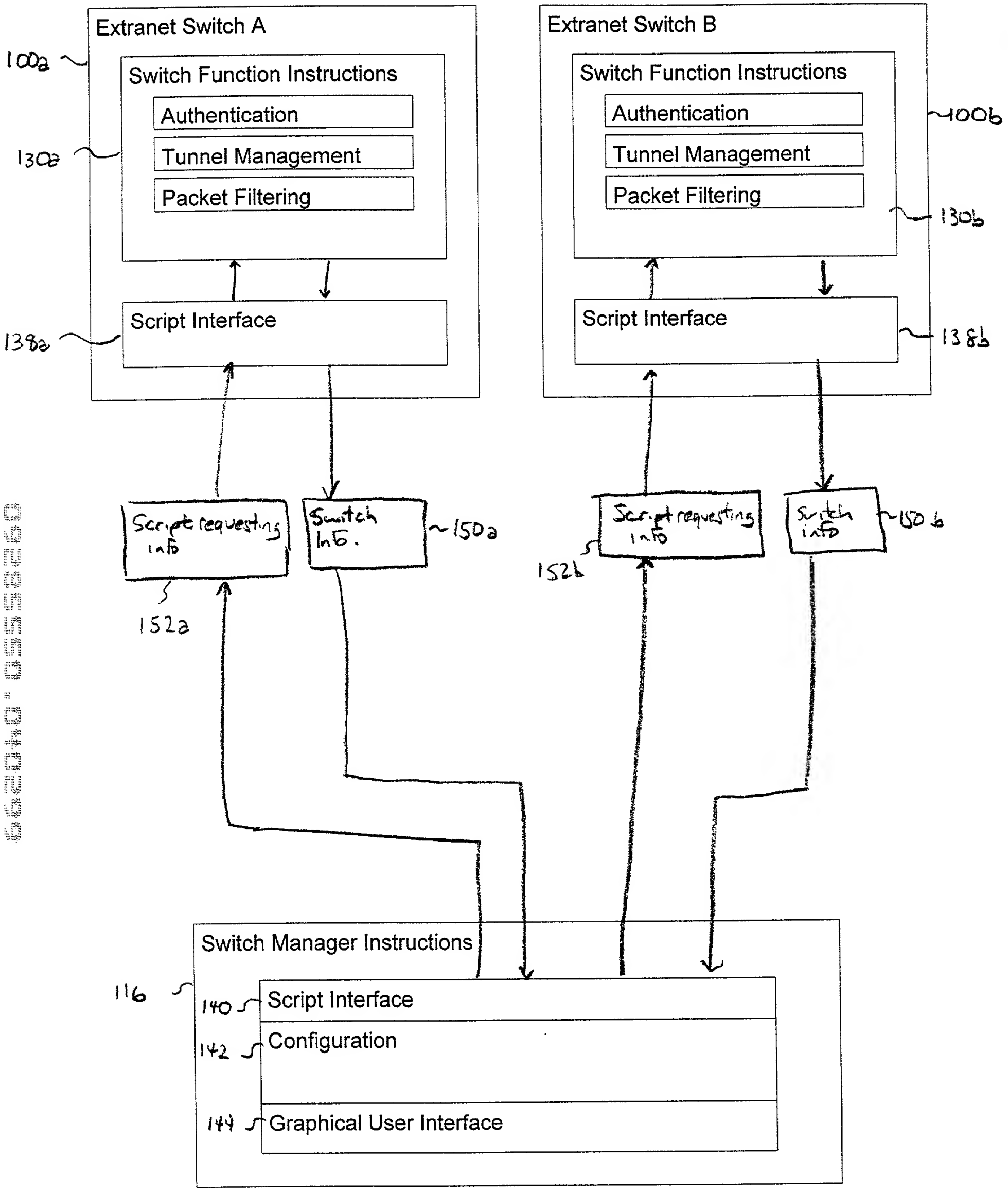
Extranet Switch A
100a
Switch Function Instructions
Authentication
Tunnel Management
Packet Filtering
130a
Script Interface
138a
Extranet Switch B
100b
Switch Function Instructions
Authentication
Tunnel Management
Packet Filtering
130b
Script Interface
138b
Script requesting info
152a
Switch Info.
150a
Script requesting info
152b
Switch info
150b
Switch Manager Instructions
116
140
Script Interface
142
Configuration
144
Graphical User Interface

FIG. 15

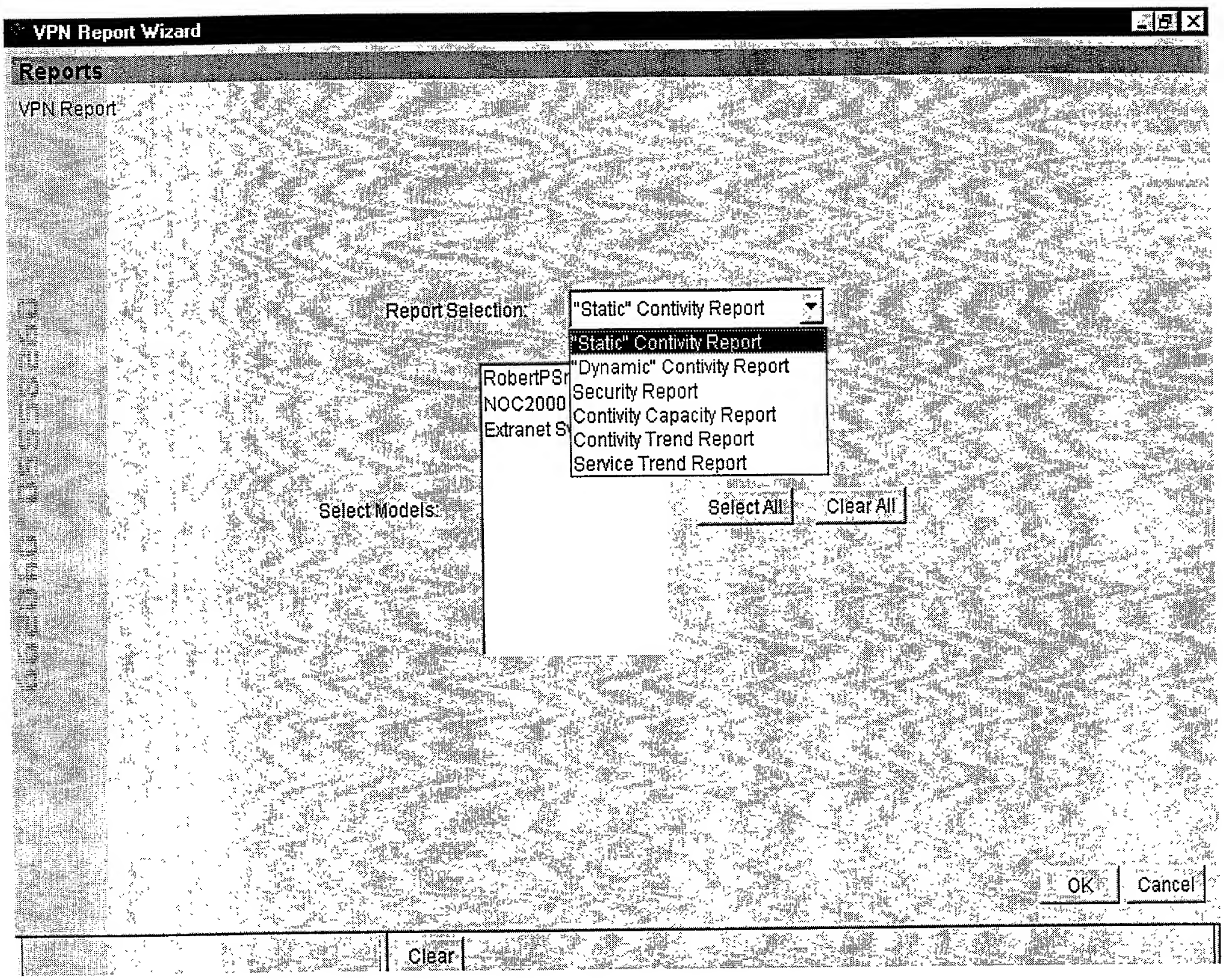
VPN Report Wizard
Reports
VPN Report
Report Selection:
"Static" Contivity Report
"Static" Contivity Report
"Dynamic" Contivity Report
Security Report
Contivity Capacity Report
Contivity Trend Report
Service Trend Report
RobertPSr
NOC2000
Extranet S
Select Models:
Select All
Clear All
OK
Cancel
Clear

FIG. 16

VPN Contivity Report

Contivity Report

Extranet switch report

Switch Name	Host Name	Domain Name	Primary Server	Secondary Server	Tertiary Server
RobertPSmack	RobertPSmack	hi.com	0.0.0.0	0.0.0.0	0.0.0.0
NOC2000	NOC2000	corpeast.baynetworks.com	132.245.135.76	132.245.135.108	0.0.0.0
Extranet Switch	*<null>*	*<null>*	*<null>*	*<null>*	*<null>*

OK Print Save

Clear

VPN Security Report

VPN Security Report

Extranet switch report

Switch Name	IPSec	PPTP	L2TP & L2F	HTTP	SNMP	FTP	TELNET	User to User	User to Branch	Branch to Branch
obertPSmack	Priv/Pub	Priv/Pub	Private	Private	Private	Private	Private	Disabled	Disabled	Disabled
NOC2000	Private	Private	Private	Private	Private	Private	Private	Enabled	Enabled	Enabled
xtranet Switch								Disabled	Disabled	Disabled

OK Print Save

Clear

FIG 18

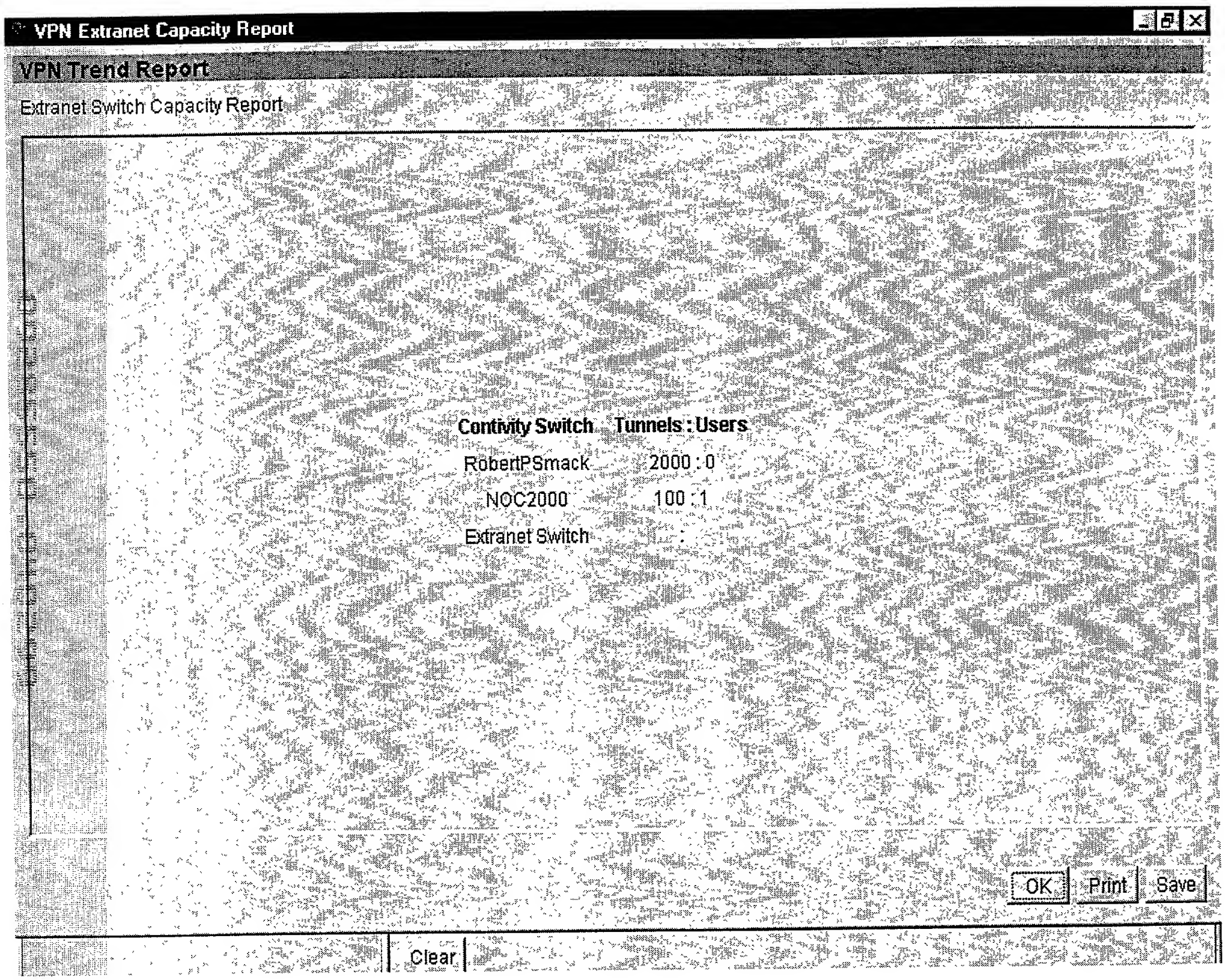
VPN Extranet Capacity Report
VPN Trend Report
Extranet Switch Capacity Report
Contivity Switch
Tunnels : Users
RobertPSmack
2000 : 0
NOC2000
100 : 1
Extranet Switch
:
OK
Print
Save
Clear

FIG. 19

VPN Contivity Trend Report

VPN Trend Report

Extranet Switch Trend Report

Dates: 1/1/99 through 3/1/99

No Sort

Contivity Switch	Total	Admin Sessions	IPSec Sessions	PPTP Sessions	L2F Sessions	L2TP Sessions
RobertPSmack	67	67	0	0	0	0
NOC2000	0	0	0	0	0	0
Extranet Switch	0	0	0	0	0	0

OK Print Save

Clear

FIG. 20

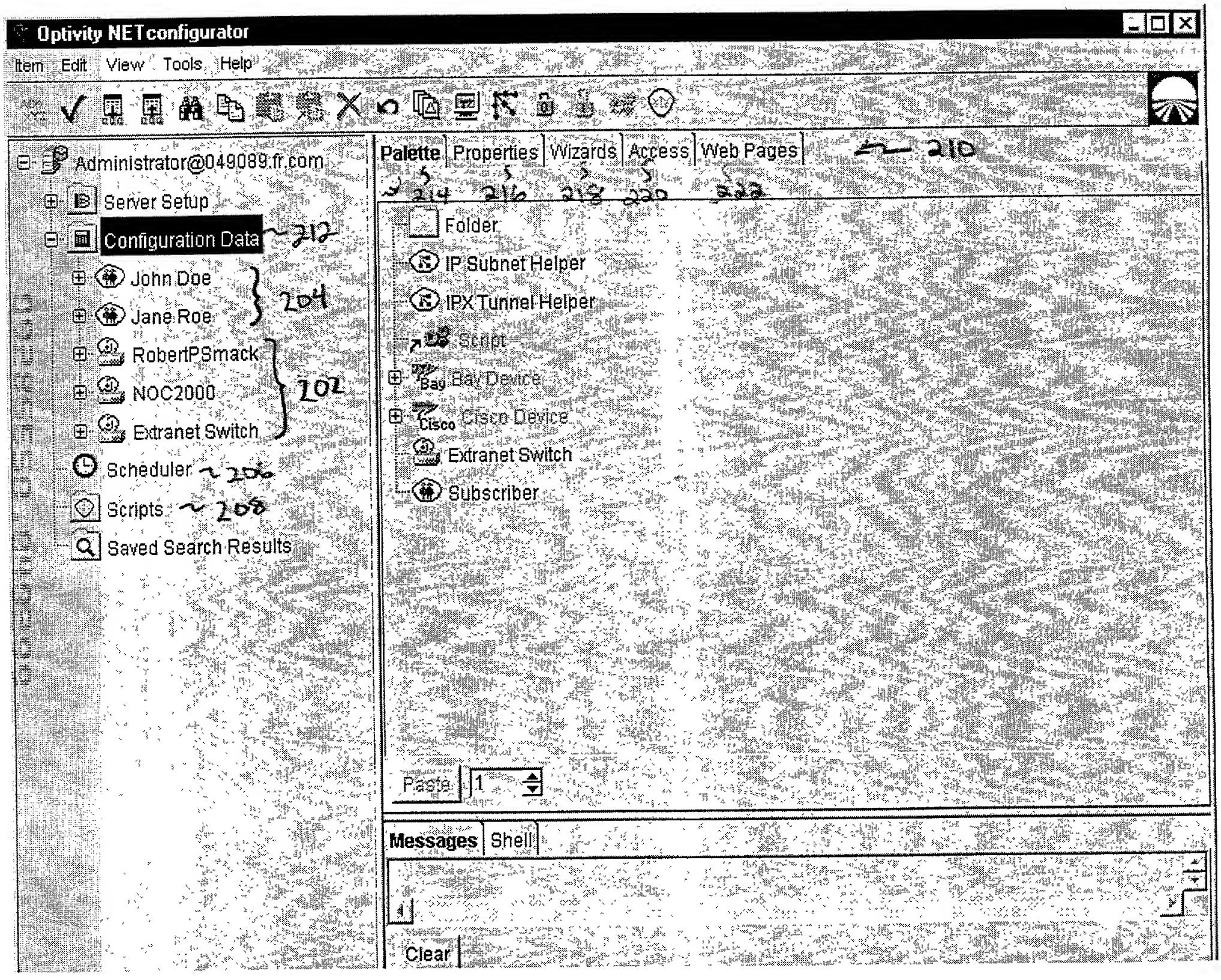
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
John Doe
Jane Roe
RobertPSmack
NOC2000
Extranet Switch
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Folder
IP Subnet Helper
IPX Tunnel Helper
Script
Bay Device
Cisco Device
Extranet Switch
Subscriber
Paste
1
Messages Shell
Clear
210
214
216
218
220
222
212
204
202
206
208
200

FIG. 21

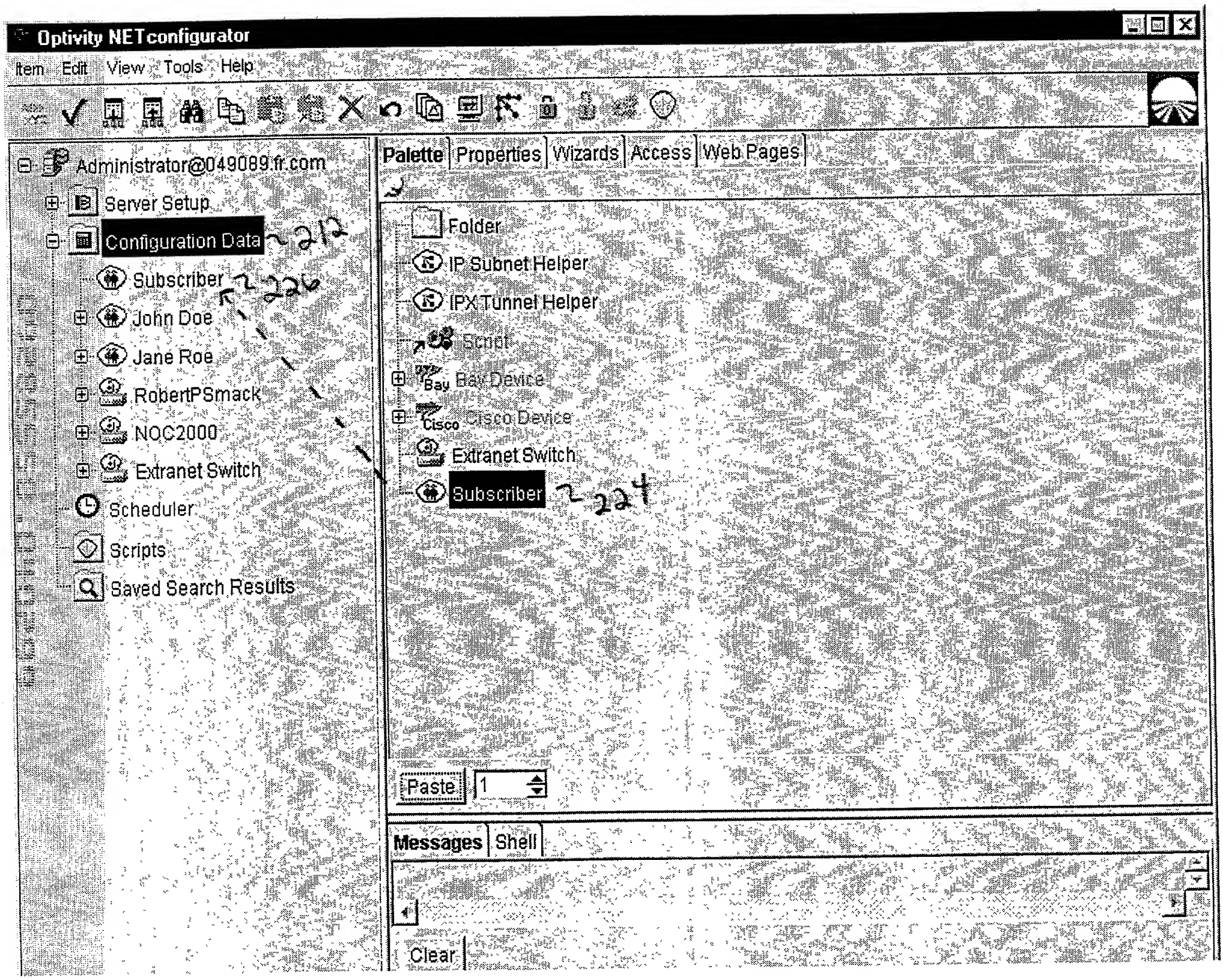
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Subscriber
John Doe
Jane Roe
RobertPSmack
NOC2000
Extranet Switch
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Folder
IP Subnet Helper
IPX Tunnel Helper
Script
Bay Device
Cisco Device
Extranet Switch
Subscriber
Paste
1
Messages Shell
Clear

FIG 22

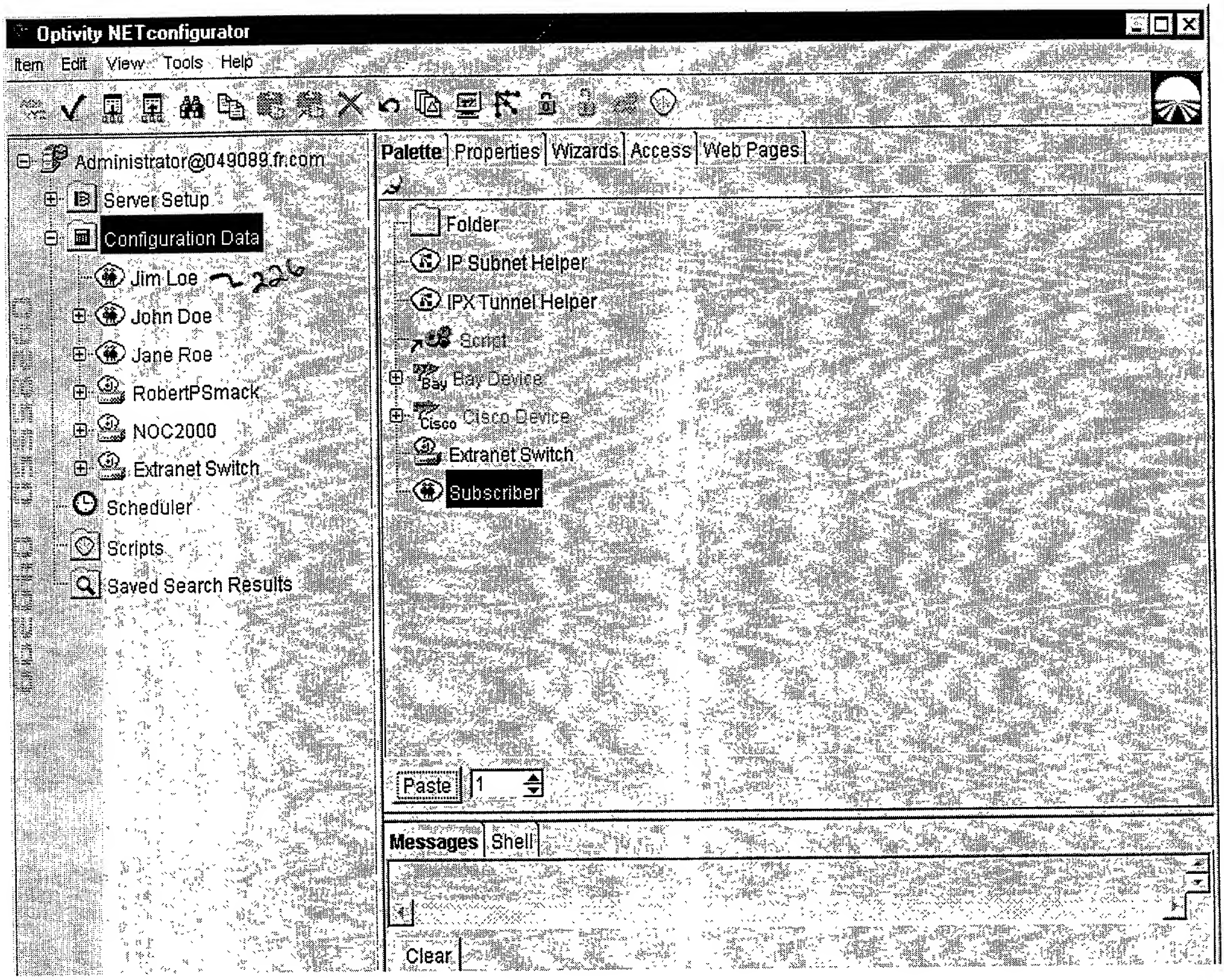
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Jim Loe
John Doe
Jane Roe
RobertPSmack
NOC2000
Extranet Switch
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Folder
IP Subnet Helper
IPX Tunnel Helper
Script
Bay Device
Cisco Device
Extranet Switch
Subscriber
Paste
1
Messages Shell
Clear

FIG 23

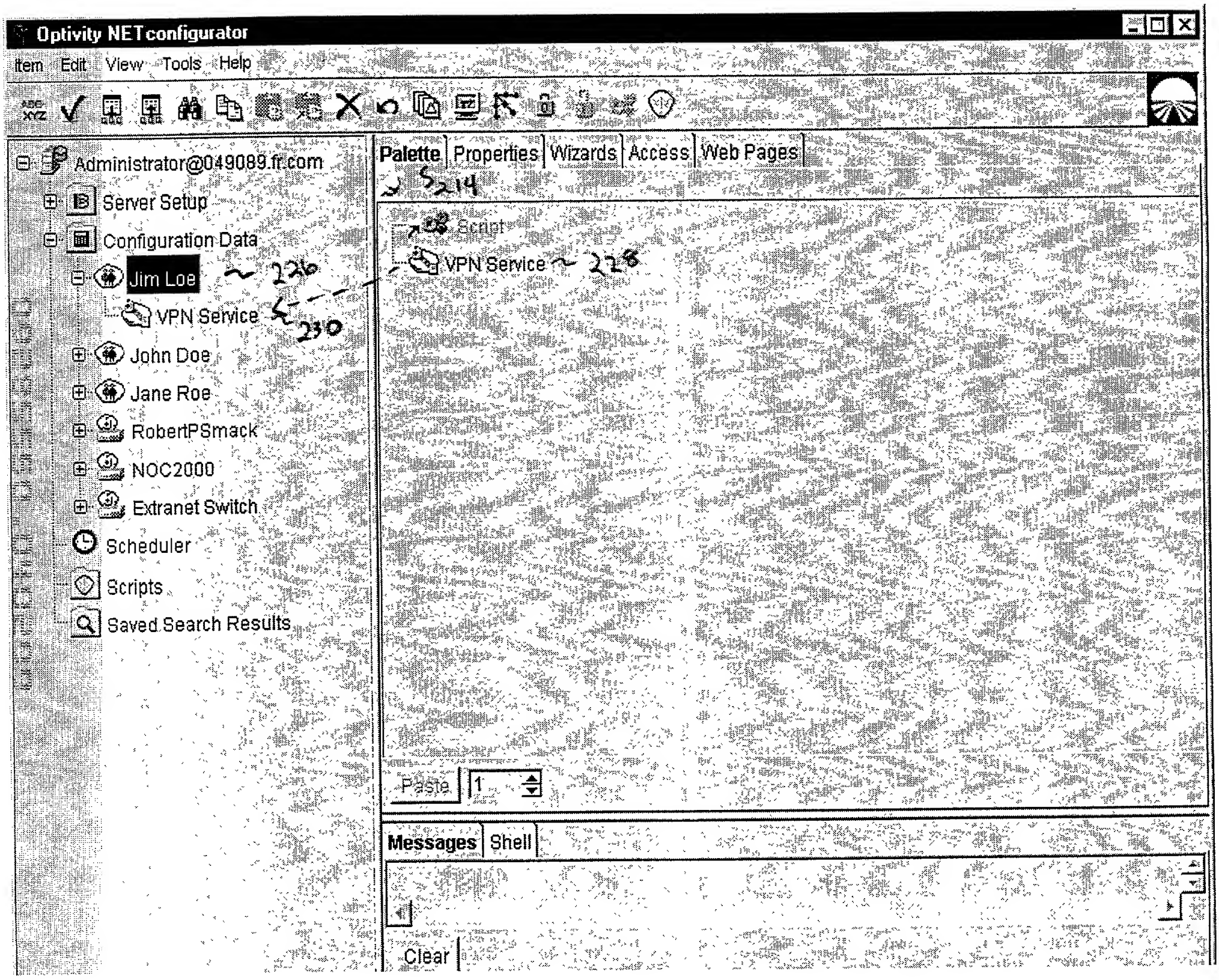
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Jim Loe
VPN Service
John Doe
Jane Roe
RobertPSmack
NOC2000
Extranet Switch
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Script
VPN Service
Paste
1
Messages Shell
Clear

FIG. 2A

Optivity NETconfigurator

Item Edit View Tools Help

Administrator@049089.fr.com
- Server Setup
- Configuration Data
  - Jim Loe
    - VPN Service 2239
  - John Doe
  - Jane Roe
  - RobertPSmack
  - NOC2000
  - Extranet Switch
- Scheduler
- Scripts
- Saved Search Results

Palette | **Properties** | Wizards | Access | Web Pages

Basic 216

Service Name: Jim's Tunnel

Tunnel Type: L2TP

IP Address: RobertPSmack

IP Address: NOC2000

IP Address of the device that the service will be using

Undo

Messages | Shell

Clear

FIG 25

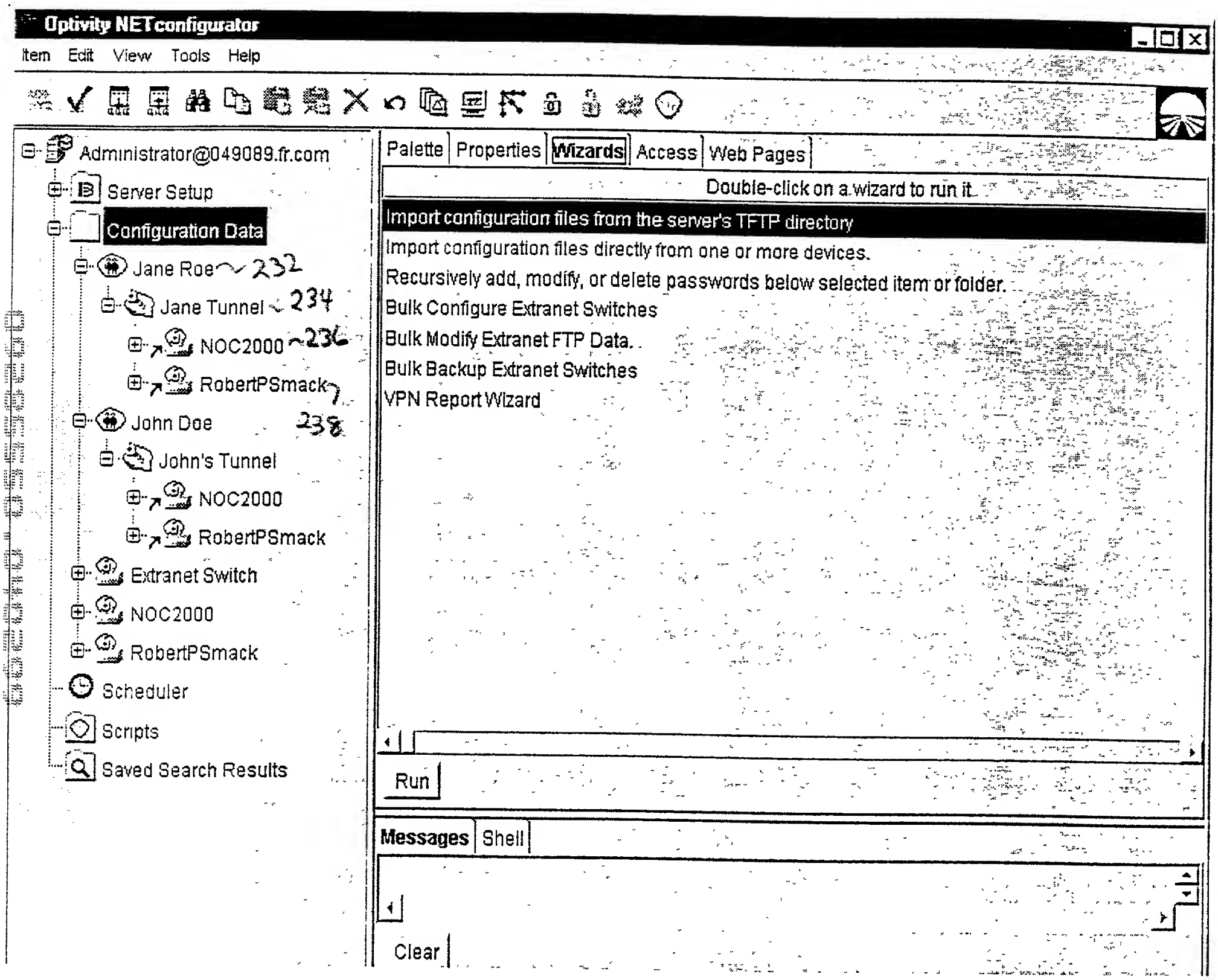
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Jane Roe ~ 232
Jane Tunnel ~ 234
NOC2000 ~ 236
RobertPSmack ~ 7
John Doe 238
John's Tunnel
NOC2000
RobertPSmack
Extranet Switch
NOC2000
RobertPSmack
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Double-click on a wizard to run it
Import configuration files from the server's TFTP directory
Import configuration files directly from one or more devices.
Recursively add, modify, or delete passwords below selected item or folder.
Bulk Configure Extranet Switches
Bulk Modify Extranet FTP Data.
Bulk Backup Extranet Switches
VPN Report Wizard
Run
Messages Shell
Clear

FIG 26

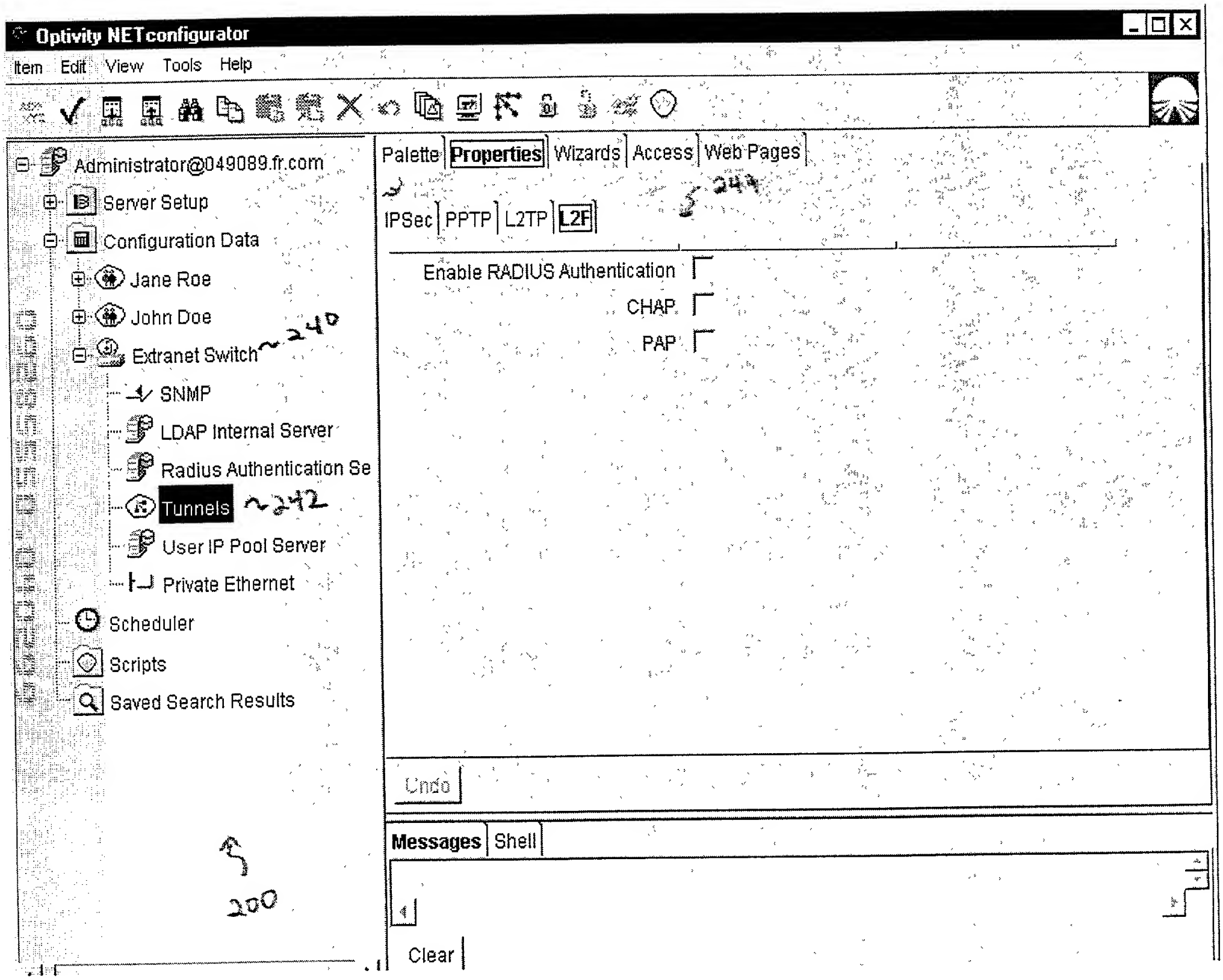
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Jane Roe
John Doe
Extranet Switch
SNMP
LDAP Internal Server
Radius Authentication Se
Tunnels
User IP Pool Server
Private Ethernet
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
IPSec PPTP L2TP L2F
Enable RADIUS Authentication
CHAP
PAP
Undo
Messages Shell
Clear

FIG 27

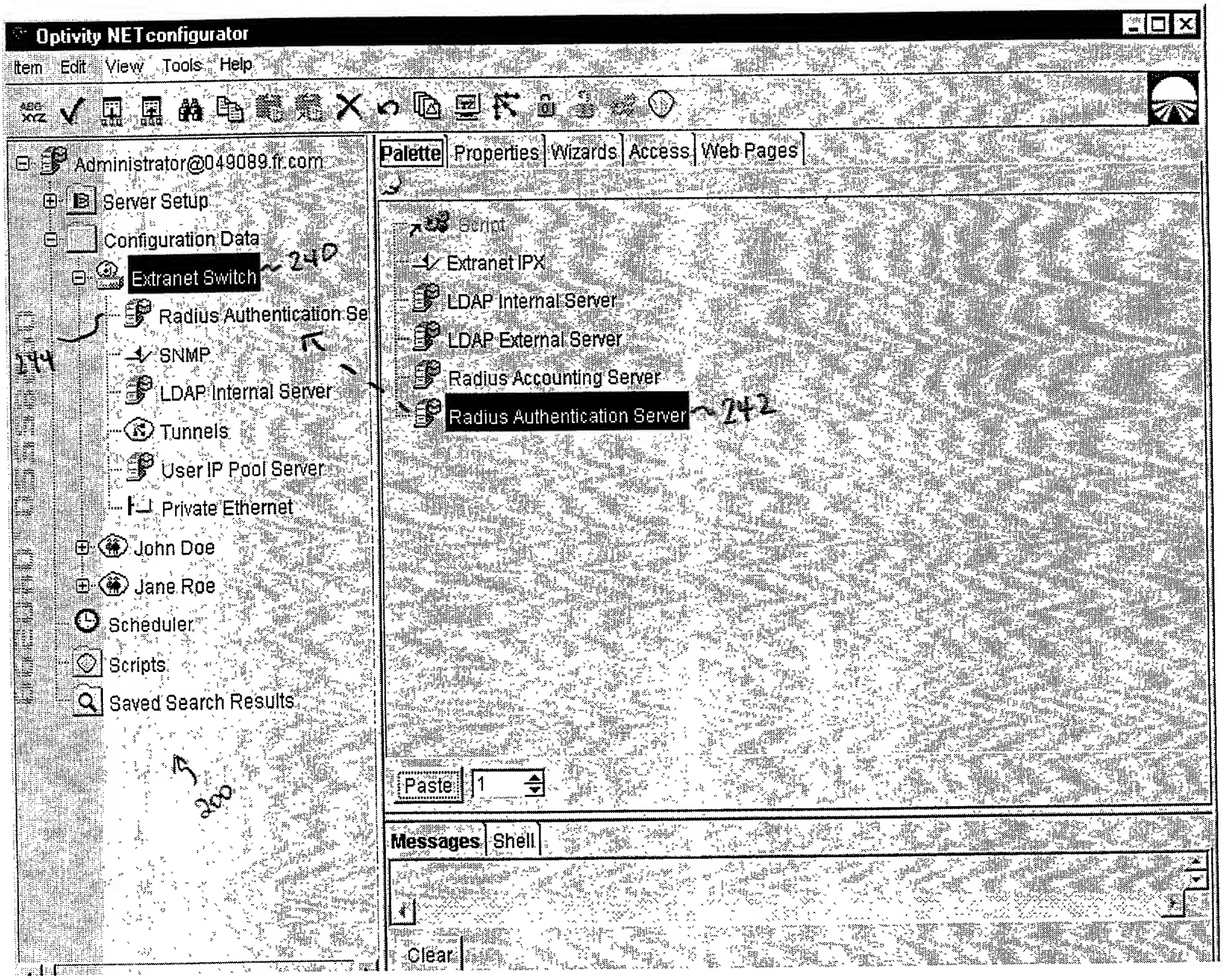
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Extranet Switch
240
Radius Authentication Se
SNMP
LDAP Internal Server
Tunnels
User IP Pool Server
Private Ethernet
John Doe
Jane Roe
Scheduler
Scripts
Saved Search Results
200
244
Palette
Properties
Wizards
Access
Web Pages
Script
Extranet IPX
LDAP Internal Server
LDAP External Server
Radius Accounting Server
Radius Authentication Server
242
Paste
1
Messages
Shell
Clear

FIG. 2B

Optivity NETconfigurator

Item Edit View Tools Help

Administrator@049089.fr.com
Server Setup
Configuration Data
Extranet Switch
Radius Authentication Se
SNMP
LDAP Internal Server
Tunnels
User IP Pool Server
Private Ethernet
John Doe
Jane Roe
Scheduler
Scripts
Saved Search Results

244

Palette | Properties | Wizards | Access | Web Pages

Basic

1 Page 1 of 2

Delimiter Value

Remove Suffix from User ID
Enable AXENT Authentication
Enable SecurID Authentication
Enable MS-CHAP Authentication
Enable CHAP Authentication
Enable PAP Authentication
Enable Primary Server
Primary Server Host Name/Address
Primary Server Port 1645
Primary Secret

Undo

Messages | Shell

Clear

FIG 29

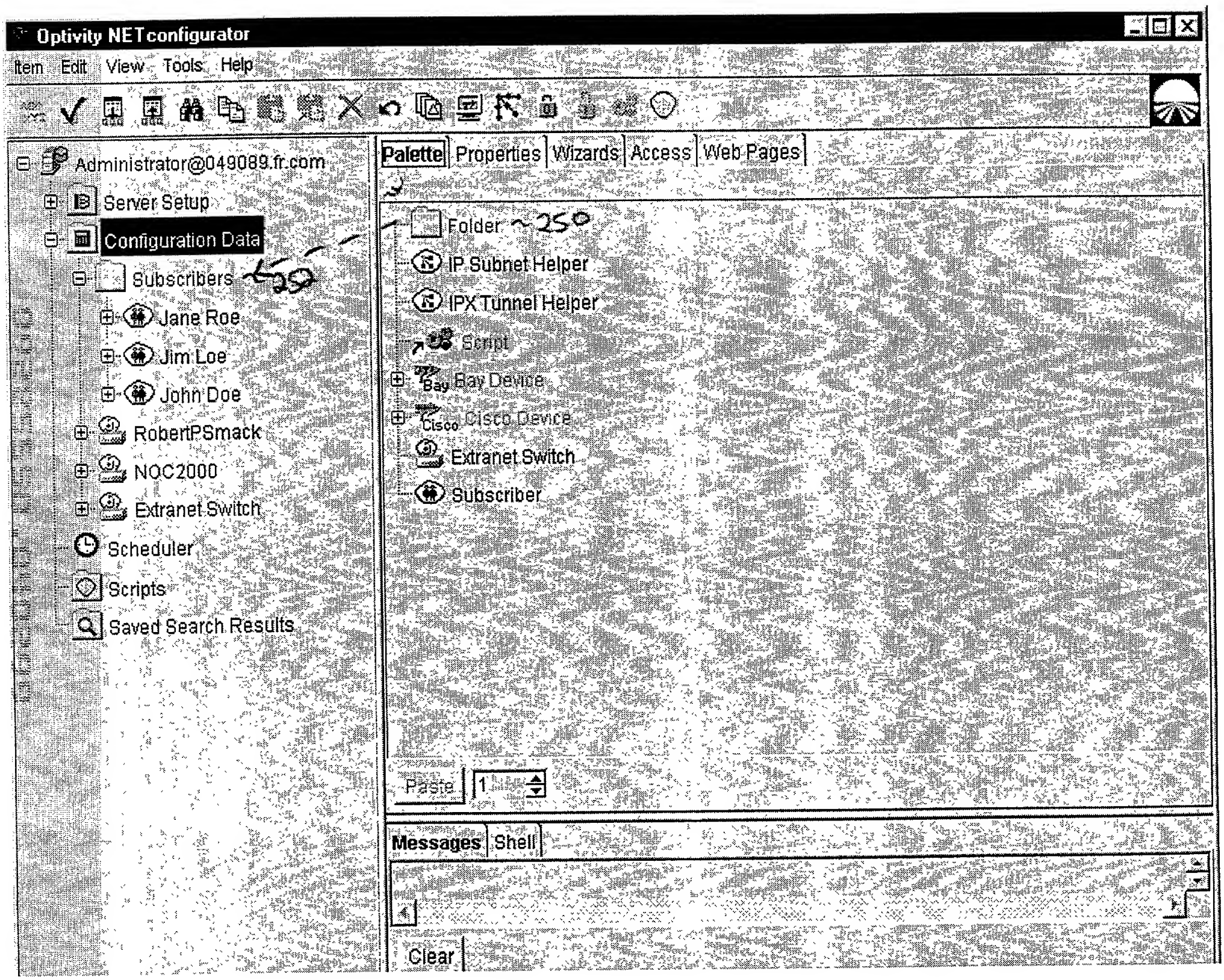
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
Subscribers
Jane Roe
Jim Loe
John Doe
RobertPSmack
NOC2000
Extranet Switch
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Folder
IP Subnet Helper
IPX Tunnel Helper
Script
Bay Device
Cisco Device
Extranet Switch
Subscriber
Paste
1
Messages Shell
Clear

FIG. 30

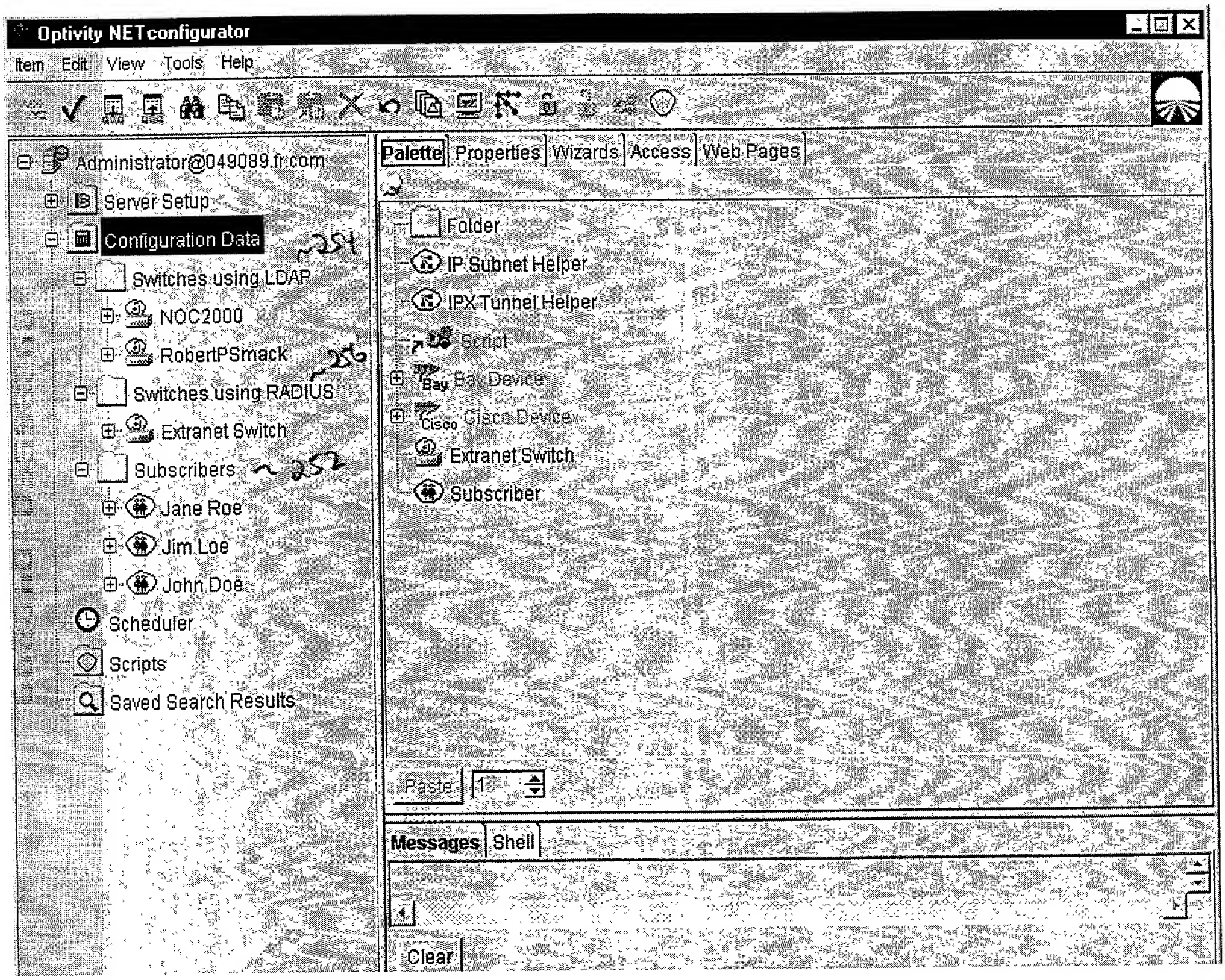
Optivity NETconfigurator
Item Edit View Tools Help
Administrator@049089.fr.com
Server Setup
Configuration Data
~254
Switches using LDAP
NOC2000
RobertPSmack
~256
Switches using RADIUS
Extranet Switch
Subscribers ~252
Jane Roe
Jim Loe
John Doe
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Folder
IP Subnet Helper
IPX Tunnel Helper
Script
Bay Bay Device
Cisco Cisco Device
Extranet Switch
Subscriber
Paste 1
Messages Shell
Clear

Fig. 3

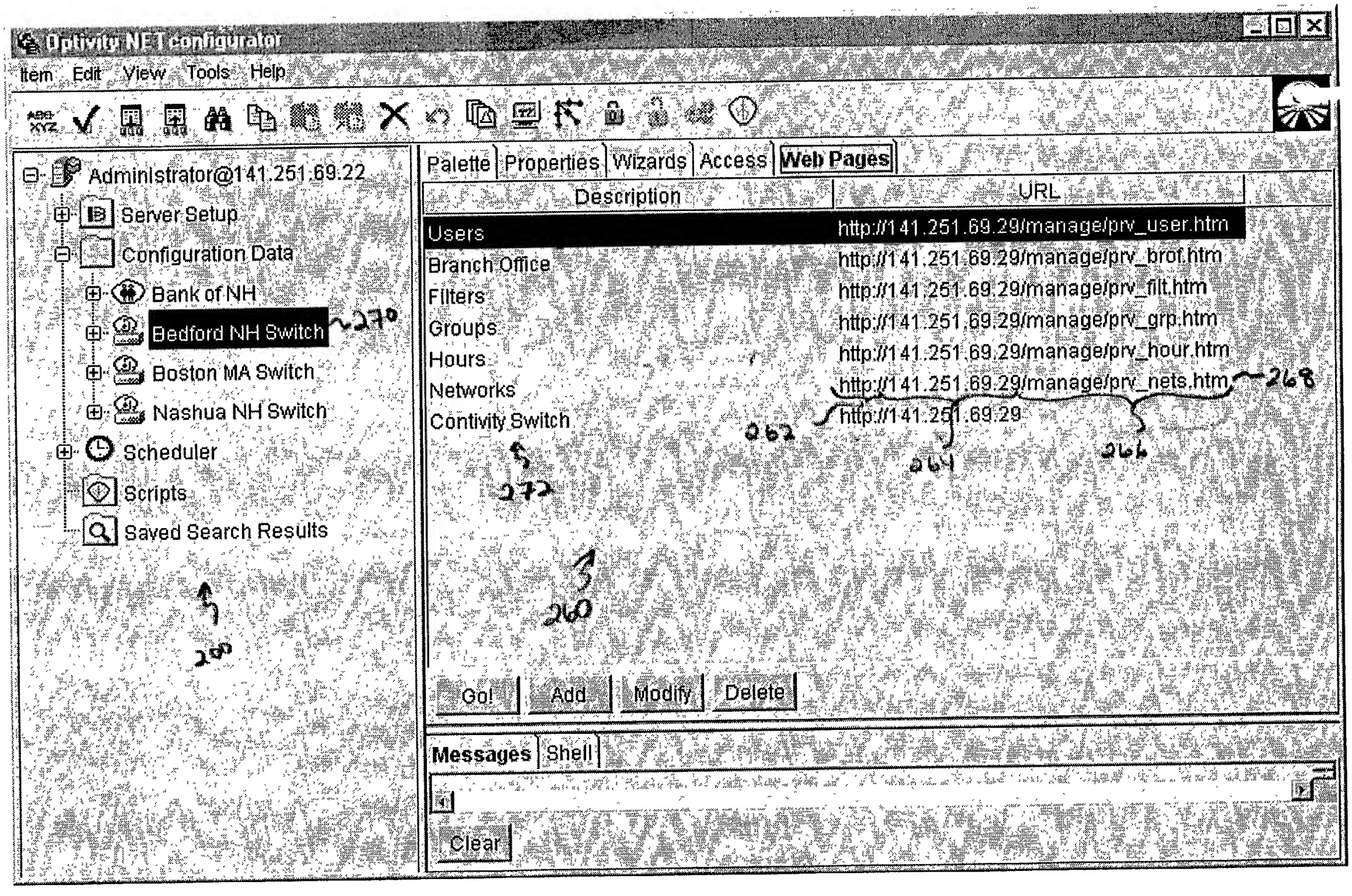
Optivity NET configurator
Item Edit View Tools Help
Administrator@141.251.69.22
Server Setup
Configuration Data
Bank of NH
Bedford NH Switch
Boston MA Switch
Nashua NH Switch
Scheduler
Scripts
Saved Search Results
Palette Properties Wizards Access Web Pages
Description
URL
Users http://141.251.69.29/manage/prv_user.htm
Branch Office http://141.251.69.29/manage/prv_brof.htm
Filters http://141.251.69.29/manage/prv_filt.htm
Groups http://141.251.69.29/manage/prv_grp.htm
Hours http://141.251.69.29/manage/prv_hour.htm
Networks http://141.251.69.29/manage/prv_nets.htm
Contivity Switch http://141.251.69.29
Go! Add Modify Delete
Messages Shell
Clear

FIG. 32

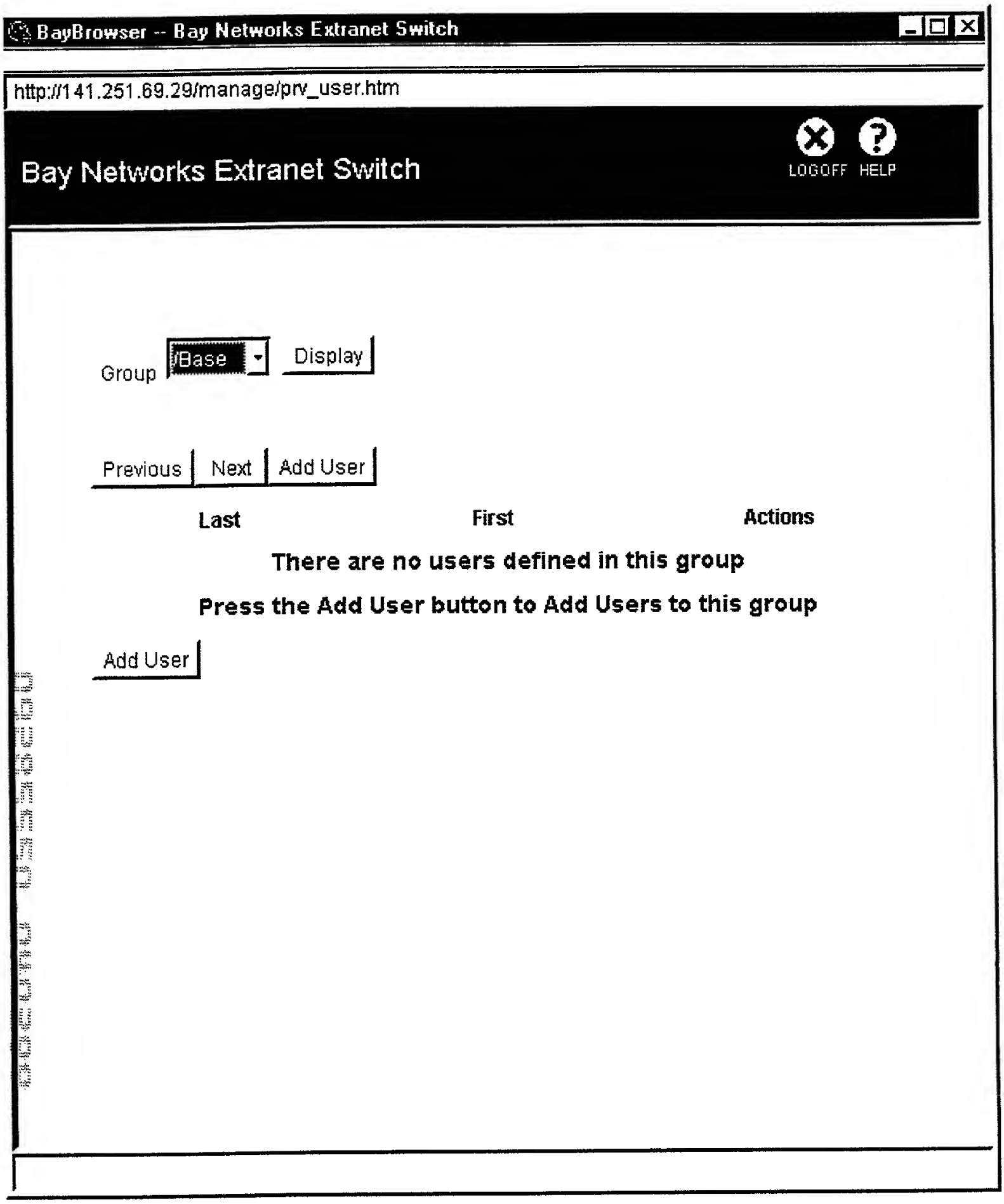
BayBrowser -- Bay Networks Extranet Switch
http://141.251.69.29/manage/prv_user.htm
Bay Networks Extranet Switch
LOGOFF
HELP
Group
/Base
Display
Previous
Next
Add User
Last
First
Actions
There are no users defined in this group
Press the Add User button to Add Users to this group
Add User

FIG. 33

BayBrowser -- Bay Networks Extranet Switch

http://141.251.69.29/manage/prv_brof.htm

Bay Networks Extranet Switch

LOGOFF HELP

/Base Edit

There are no connections defined

Press the Define Branch Office Connection button to Define Connections

Define Branch Office Connection | Add Group

FIG. 34

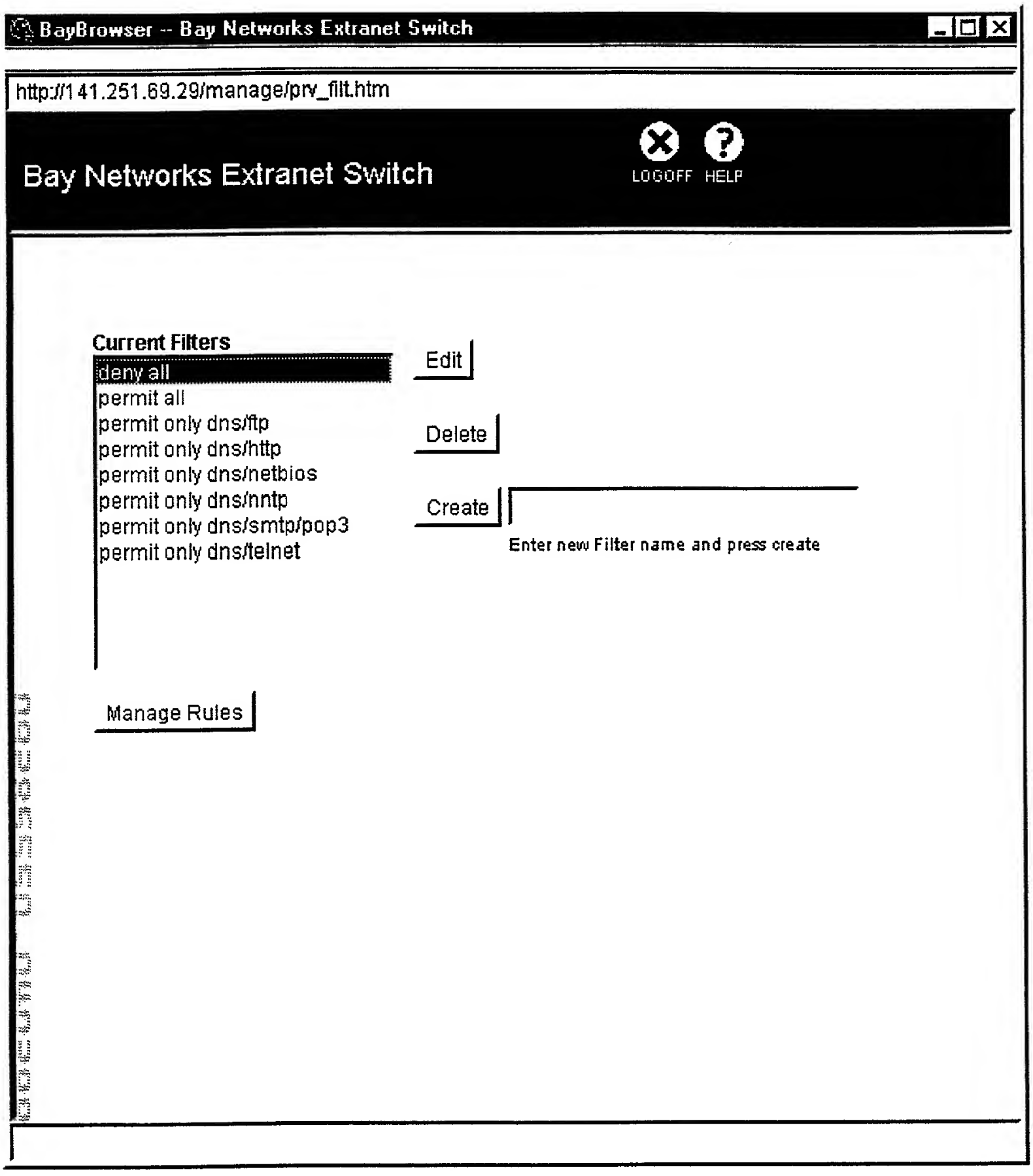
BayBrowser -- Bay Networks Extranet Switch
http://141.251.69.29/manage/prv_filt.htm
Bay Networks Extranet Switch
LOGOFF
HELP
Current Filters
deny all
permit all
permit only dns/ftp
permit only dns/http
permit only dns/netbios
permit only dns/nntp
permit only dns/smtp/pop3
permit only dns/telnet
Edit
Delete
Create
Enter new Filter name and press create
Manage Rules

FIG. 3,5

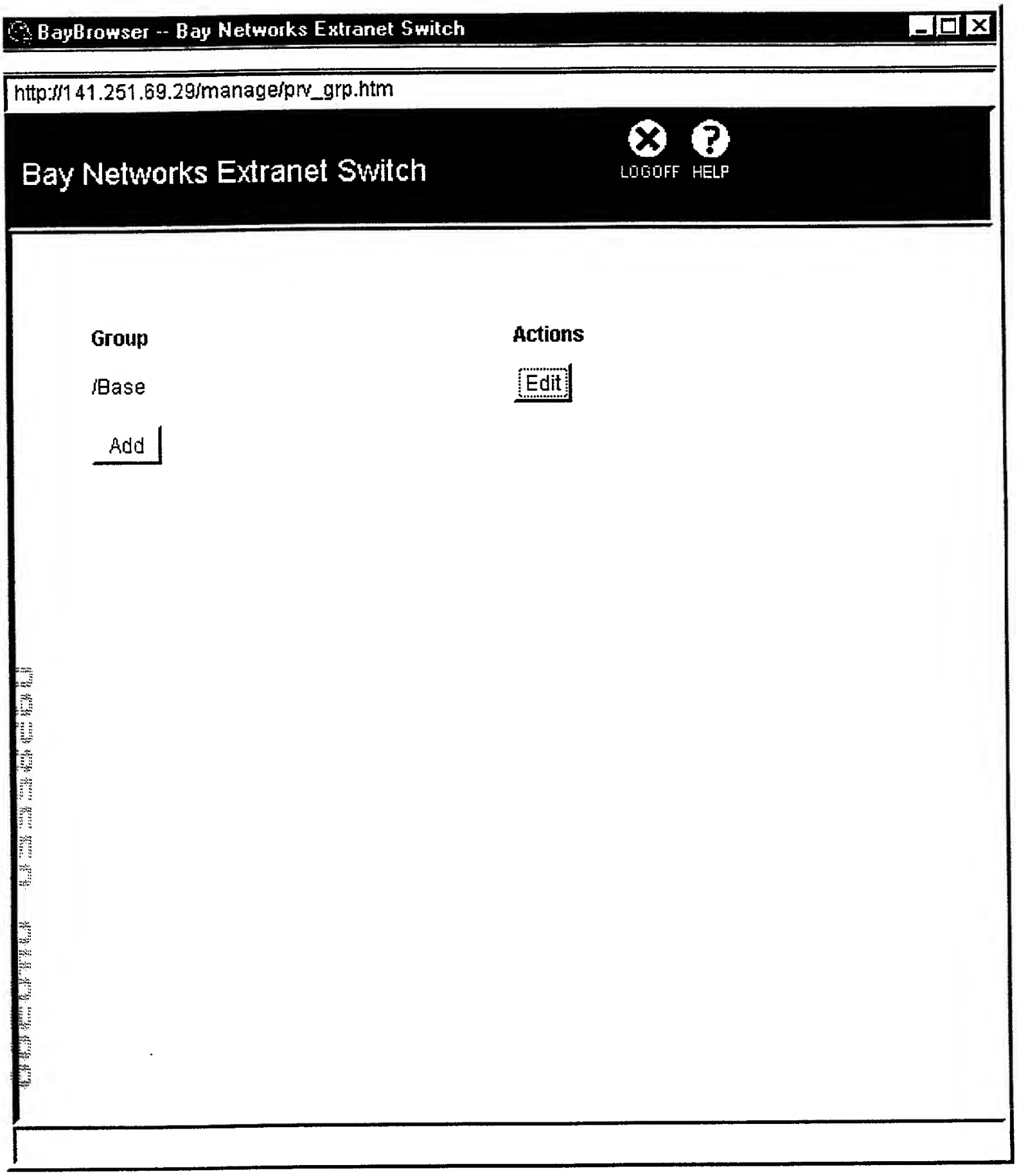
BayBrowser -- Bay Networks Extranet Switch
http://141.251.69.29/manage/prv_grp.htm
Bay Networks Extranet Switch
LOGOFF
HELP
Group
Actions
/Base
Edit
Add

FIG. 36

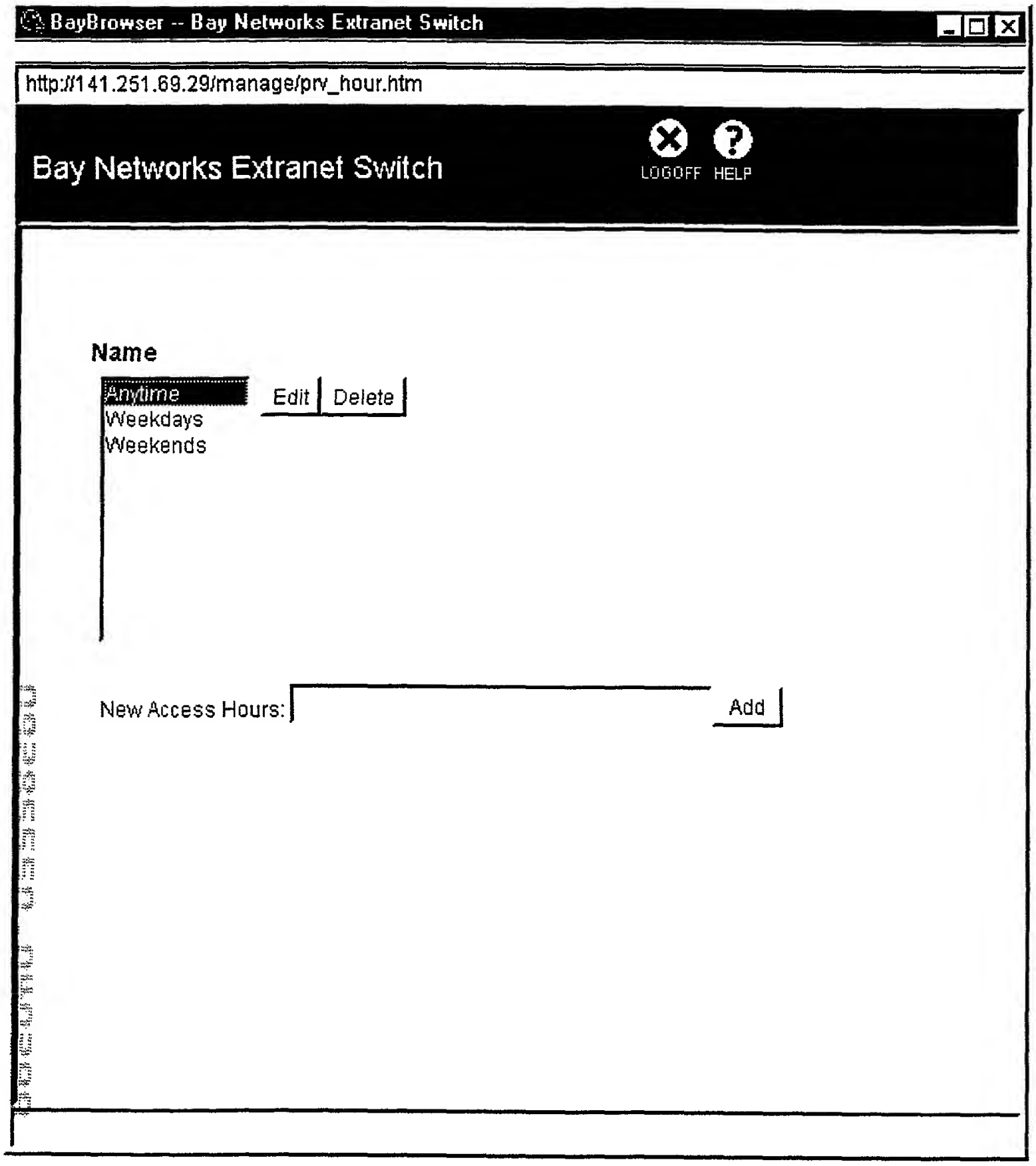
BayBrowser -- Bay Networks Extranet Switch
http://141.251.69.29/manage/prv_hour.htm
Bay Networks Extranet Switch
LOGOFF
HELP
Name
Anytime
Weekdays
Weekends
Edit
Delete
New Access Hours:
Add

FIG. 37

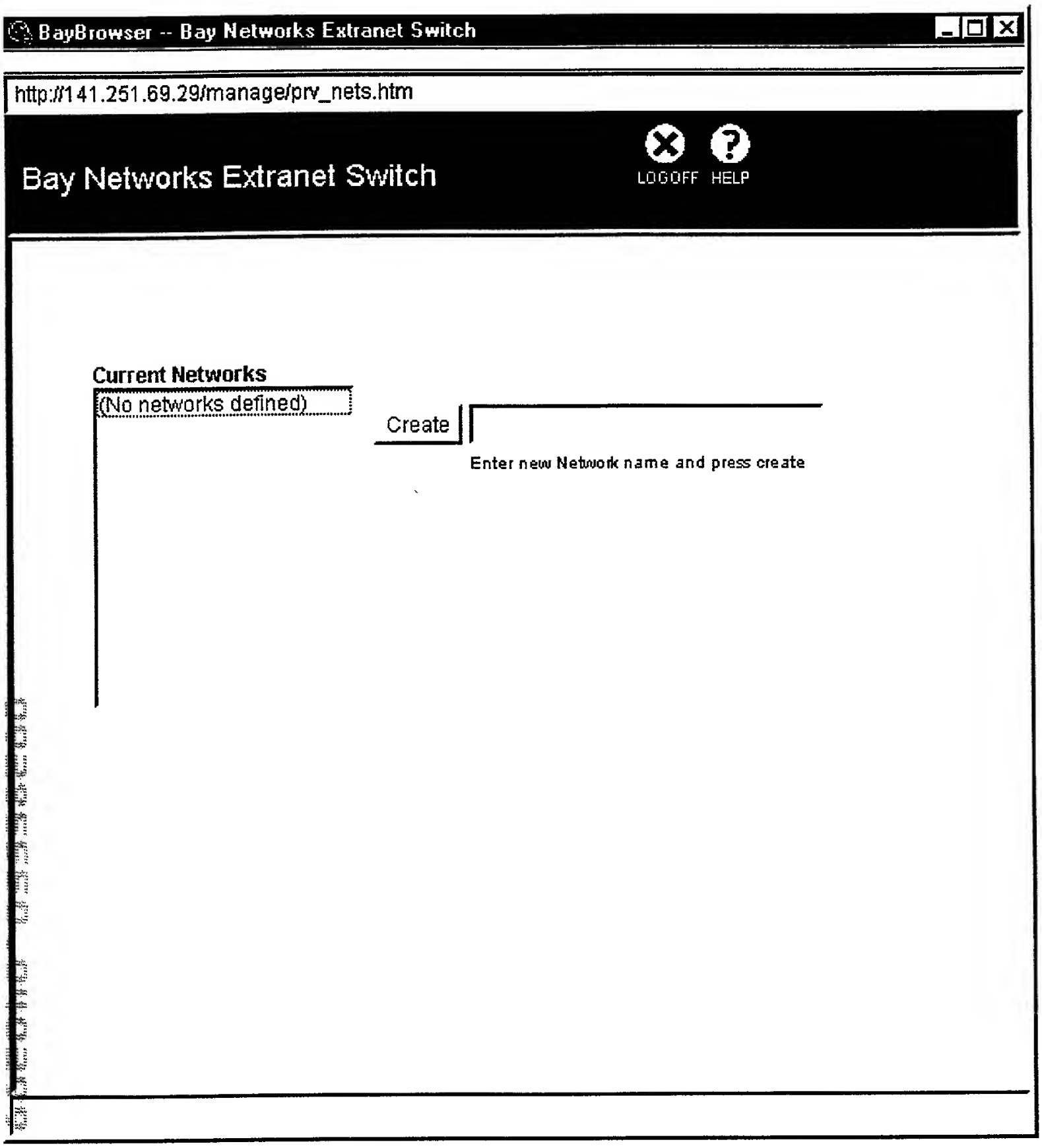
BayBrowser -- Bay Networks Extranet Switch
http://141.251.69.29/manage/prv_nets.htm
Bay Networks Extranet Switch
LOGOFF
HELP
Current Networks
(No networks defined)
Create
Enter new Network name and press create

FIG. 38

BayBrowser -- Connecting...

http://141.251.69.29/

Welcome to the Bay Networks Extranet Switch

Ongoing Management

MANAGE SWITCH

MANAGE SWITCH - The management interface used for the day-to-day management and monitoring of the Extranet Switch.

MANAGE from NOTEBOOK

MANAGE from NOTEBOOK - Reduced graphics version of the management interface. Excellent for small monitors and notebook PCs.

Getting Started

QUICK START

QUICK START - A great way to get your new Extranet Switch up and running in just minutes. By completing just a single set-up screen, you can configure the Extranet Switch to support PPTP tunnels.

GUIDED CONFIG

GUIDED CONFIG - Guides you through the entire management interface, providing hints on how to configure the extensive list of features.

FIG. 39

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled MONITORING A VIRTUAL PRIVATE NETWORK, the specification of which

- ■ is attached hereto.
- ☐ was filed on _____ as Application Serial No. _____ and was amended on _____.
- ☐ was described and claimed in PCT International Application No. _____ filed on _____ and as amended under PCT Article 19 on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information I know to be material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: Denis G. Maloney, Reg. No. 29,670; David L. Feigenbaum, Reg. No. 30,378; Timothy A. French, Reg. No. 30,175; Cathy L. Peterson, Reg. No. 41,249; Robert A. Greenberg, Reg. No. 44,133.

Address all telephone calls to Denis G. Maloney at telephone number 617/542-5070.

Address all correspondence to Denis G. Maloney, Fish & Richardson P.C., 225 Franklin Street , Boston, MA 02110-2804.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Full Name of Inventor: Matthew W. Poisson

Inventor's Signature: _____ Date: _____

Residence Address: Manchester, New Hampshire

Citizen of: USA

Post Office Address: Manchester, New Hampshire

COMBINED DECLARATION AND POWER OF ATTORNEY CONTINUED

Full Name of Inventor: Melissa L. Desroches

Inventor's Signature: _____ Date: _____

Residence Address: Kingston, New Hampshire

Citizen of: USA

Post Office Address: Kingston, New Hampshire

Full Name of Inventor: James M. Milillo

Inventor's Signature: _____ Date: _____

Residence Address: Manchester, New Hampshire

Citizen of: USA

Post Office Address: Manchester, New Hampshire

Full Name of Inventor: Ravi Subbarao

Inventor's Signature: _____ Date: _____

Residence Address: Bedford, New Hampshire

Citizen of: USA

Post Office Address: Bedford, New Hampshire

365890.B11